Horizon 7 安装指南

2019 年 3 月 14 日
VMware Horizon 7 7.8

vmware®

您可以从 VMware 网站下载最新的技术文档：
https://docs.vmware.com/cn/。
VMware 网站还提供了最近的产品更新。
如果您对本文档有任何意见或建议，请将反馈信息发送至：
docfeedback@vmware.com

VMware, Inc.
3401 Hillview Ave.
Palo Alto, CA 94304
www.vmware.com

北京办公室
北京市
朝阳区新源南路 8 号
启皓北京东塔 8 层 801
www.vmware.com/cn

上海办公室
上海市
淮海中路 333 号
瑞安大厦 804-809 室
www.vmware.com/cn

广州办公室
广州市
天河路 385 号
太古汇一座 3502 室
www.vmware.com/cn

目录

Horizon 7 安装 6

1 服务器组件的系统要求 7
- Horizon 连接服务器的要求 7
- Horizon Administrator 要求 9
- View Composer 的要求 9

2 客户机操作系统的系统要求 12
- Horizon Agent 支持的操作系统 12
- 独立 Horizon Persona Management 支持的操作系统 13
- 远程显示协议和软件支持 13

3 在 IPv6 环境中安装 Horizon 7 19
- 在 IPv6 环境中设置 Horizon 7 19
- IPv6 环境中支持的 vSphere 数据库和 Active Directory 版本 20
- IPv6 环境中 Horizon 7 Server 支持的操作系统 20
- IPv6 环境中桌面和 RDS 主机支持的 Windows 操作系统 21
- IPv6 环境中支持的客户端 21
- IPv6 环境中支持的远程协议 21
- IPv6 环境中支持的身份验证类型 22
- IPv6 环境中其他受支持的功能 22

4 以 FIPS 模式安装 Horizon 7 25
- 以 FIPS 模式安装 Horizon 7 的概述 25
- FIPS 模式的系统要求 26

5 准备 Active Directory 27
- 配置域和信任关系 27
- 为远程桌面创建 OU 28
- 为 Kiosk 模式客户端帐户创建组织单位和组 29
- 创建用户组 29
- 为 vCenter Server 创建用户帐户 29
- 为独立的 View Composer Server 创建用户帐户 29
- 为 View Composer AD 操作创建用户帐户 30
- 为即时克隆操作创建用户帐户 31
- 配置受限制的组策略 31
- 使用 Horizon 7 组策略管理模板文件 32
- 为智能卡身份验证准备 Active Directory 32

在 SSL/TLS 中禁用弱密码 35

6 安装 View Composer 37
准备 View Composer 数据库 37
为 View Composer 配置 SSL 证书 45
安装 View Composer 服务 45
对从 View Composer 进行的 vCenter 和 ESXi 连接启用 TLSv1.0 47
为 View Composer 配置基础架构 48

7 安装 Horizon 连接服务器 50
安装 Horizon 连接服务器软件 50
安装 Horizon 连接服务器的前提条件 51
使用新配置安装 Horizon 连接服务器 51
安装 Horizon 连接服务器副本实例 58
配置安全服务器的配对密码 64
安装安全服务器 65
Unified Access Gateway 设备优于 VPN 的方面 72
Horizon 连接服务器的防火墙规则 73
使用备份配置重新安装 Horizon 连接服务器 75
Microsoft Windows Installer 命令行选项 76
使用 MSI 命令行选项静默卸载 Horizon 7 组件 77

8 为 Horizon 7 Server 配置 TLS 证书 80
了解 Horizon 7 Server 的 TLS 证书 80
TLS 证书设置任务概述 82
获取 CA 签发的 TLS 证书 83
配置 Horizon 连接服务器、安全服务器或 View Composer 以使用新 TLS 证书 84
配置客户端端点以信任根证书和中间证书 89
为服务器证书配置证书撤消检查 91
配置 PCoIP 安全网关以使用新 TLS 证书 92
将 Horizon Administrator 设置为信任 vCenter Server 或 View Composer 证书 96
使用 CA 签发的 TLS 证书的优势 96
Horizon 连接服务器和安全服务器上的证书问题故障排除 96

9 为订阅许可证启用 Horizon 7 98
VMware Horizon 7 Cloud Connector 98
使用 Horizon 7 部署 Horizon 7 Cloud Connector 虚拟设备 98
为 Horizon 7 Cloud Connector root 用户设置密码到期策略 100
为 Horizon 7 Cloud Connector 虚拟设备配置 CA 签名的证书 101

10 首次配置 Horizon 7 103

为 vCenter Server、View Composer 和即时克隆配置用户帐户 103

首次配置 Horizon 连接服务器 108

配置 Horizon Client 连接 119

替换 Horizon 7 服务的默认端口 127

调整 Windows Server 设置以支持您的部署 132

11 配置事件报告 134

为 Horizon 7 事件添加数据库和数据库用户 134

为事件报告准备 SQL Server 数据库 135

配置事件数据库 135

为 Syslog 服务器配置事件日志记录 137

Horizon 7 安装

《Horizon 7 安装指南》介绍如何安装 VMware Horizon® 7 服务器和客户端组件。

目标读者

本文档所述信息面向所有想要安装 VMware Horizon 7 的人员。本文档中的信息专门为已熟练掌握虚拟机技术和数据中心操作、并具有丰富经验的 Windows 或 Linux 系统管理员编写。

服务器组件的系统要求

1

运行 Horizon 7 server 组件的主机必须满足特定的硬件和软件要求。

本章讨论了以下主题：

- Horizon 连接服务器的要求
- Horizon Administrator 要求
- View Composer 的要求

Horizon 连接服务器的要求

Horizon 连接服务器充当客户端连接代理，负责执行身份验证并将传入的用户请求定向到相应的远程桌面和应用程序。Horizon 连接服务器具有特定的硬件、操作系统、安装和支持软件要求。

- Horizon 连接服务器的硬件要求

  您必须在满足特定硬件要求的专用物理机或虚拟机上安装所有 Horizon 连接服务器安装类型（包括标准服务器、副本服务器、安全服务器和注册服务器安装）。

- Horizon 连接服务器支持的操作系统

  您必须在支持的 Windows Server 操作系统上安装 Horizon 连接服务器。

- Horizon 连接服务器的虚拟化软件要求

  Horizon 连接服务器要求使用特定版本的 VMware 虚拟化软件。

- Horizon 连接服务器副本实例的网络要求

  在安装 Horizon 连接服务器副本实例时，通常必须在相同物理位置配置这些实例并通过高性能 LAN 连接这些实例。否则，延迟问题会导致 Horizon 连接服务器实例上的 View LDAP 配置不一致。用户在连接配置过时的 Horizon 连接服务器实例时，可能会被拒绝访问。

Horizon 连接服务器的硬件要求

您必须在满足特定硬件要求的专用物理机或虚拟机上安装所有 Horizon 连接服务器安装类型（包括标准服务器、副本服务器、安全服务器和注册服务器安装）。

表 1-1. Horizon 连接服务器的硬件要求

硬件组件	需要	建议
处理器	Pentium IV 2.0 GHz 处理器或更高	4 个 CPU
网络适配器	100Mbps 网卡	1 Gbps 网卡
内存 Windows Server 2008 R2 (64 位)	4GB RAM 或更高	至少 10GB RAM，可部署 50 个或更多远程桌面
内存 Windows Server 2012 R2 (64 位)	4GB RAM 或更高	至少 10GB RAM，可部署 50 个或更多远程桌面

这些要求也适用于您针对高可用性或外部访问安装的其他 Horizon 连接服务器副本服务器和安全服务器实例。

重要 托管 Horizon 连接服务器的物理机或虚拟机必须具有不会发生更改的 IP 地址。在 IPv4 环境中，配置静态 IP 地址。在 IPv6 环境中，计算机会自动获取不会发生更改的 IP 地址。

Horizon 连接服务器支持的操作系统

您必须在支持的 Windows Server 操作系统上安装 Horizon 连接服务器。

以下操作系统支持所有 Horizon 连接服务器安装类型，包括标准服务器、副本服务器和安全服务器的安装。

表 1-2. Horizon 连接服务器的操作系统支持

操作系统	版本	功能版本
Windows Server 2008 R2 SP1	64 位	Standard Enterprise Datacenter
Windows Server 2012 R2	64 位	Standard Datacenter
Windows Server 2016	64 位	Standard Datacenter

注 不再支持无 Service Pack 的 Windows Server 2008 R2。

Horizon 连接服务器的虚拟化软件要求

Horizon 连接服务器要求使用特定版本的 VMware 虚拟化软件。

如果使用 vSphere，则必须使用受支持的 vSphere ESX/ESXi 主机和 vCenter Server 版本。

有关哪些 Horizon 版本与哪些 vCenter Server 和 ESXi 版本相兼容的详细信息，请参阅《VMware 产品互操作性列表》，其网址为 http://www.vmware.com/resources/compatibility/sim/interop_matrix.php。

Horizon 连接服务器副本实例的网络要求

在安装 Horizon 连接服务器副本实例时，通常必须在相同物理位置配置这些实例并通过高性能 LAN 连接这些实例。否则，延迟问题会导致 Horizon 连接服务器实例上的 View LDAP 配置不一致。用户在连接配置过时的 Horizon 连接服务器实例时，可能会被拒绝访问。

重要 要在 WAN、MAN（城域网）或其他非 LAN 中使用连接服务器的一组副本实例，如果 Horizon 部署需要跨多个数据中心，则必须使用 Cloud Pod 架构功能。有关更多信息，请参阅《在 Horizon 7 中管理 Cloud Pod 架构》文档。

Horizon Administrator 要求

管理员可使用 Horizon Administrator 配置 Horizon Connection Server、部署和管理远程桌面和应用程序、控制用户身份验证、启动并检查系统事件以及执行分析活动。运行 Horizon Administrator 的客户端系统必须满足特定要求。

Horizon Administrator 是一种基于 Web 的应用程序，会随连接服务器一起安装。您可以通过以下 Web 浏览器访问和使用 Horizon Administrator：

- Internet Explorer 9（不建议）
- Internet Explorer 10
- Internet Explorer 11
- Firefox（受支持的最新版本）
- Chrome（受支持的最新版本）
- Safari 6 和更高版本
- Microsoft Edge (Windows 10)

要通过 Web 浏览器使用 Horizon Administrator，您必须安装 Adobe Flash Player 10.1 或更高版本。客户端系统必须具有访问 Internet 的权限，才能安装 Adobe Flash Player。

用于启动 Horizon Administrator 的计算机必须信任托管连接服务器的服务器的根证书和中间证书。支持的浏览器已包含所有公认证书颁发机构 (CA) 的证书。如果您的证书来自非知名的 CA，则必须遵循配置客户端端点以信任根证书和中间证书中的说明。

要正确显示文本，需要为 Horizon Administrator 安装 Microsoft 特定的字体。如果您的 Web 浏览器在非 Windows 操作系统（如 Linux、UNIX 或 Mac）上运行，请确保在您的计算机上安装了 Microsoft 特定的字体。

目前，Microsoft 网站不提供 Microsoft 字体，但您可以从其他独立网站进行下载。

View Composer 的要求

您可以借助 View Composer 从单个集中式基础映像部署多个链接克隆桌面。View Composer 具有特定的安装和存储要求。

- View Composer 支持的操作系统

  View Composer 支持 64 位操作系统，但具有特定要求和限制。可以在与 vCenter Server 相同的物理机或虚拟机或者一个单独的服务器上安装 View Composer。

- 独立 View Composer 的硬件要求

  如果通过用于 vCenter Server 的物理机或虚拟机将 View Composer 安装在其他物理机或虚拟机上，则必须使用可满足特定硬件要求的专用计算机。

- View Composer 和事件数据库的数据库要求

  View Composer 需要使用 SQL 数据库来存储数据。View Composer 数据库必须位于 View Composer server 主机上，或者能够供其使用。（可选）您可以设置事件数据库以记录来自 Horizon Connection Server 的有关 Horizon 事件的信息。

View Composer 支持的操作系统

View Composer 支持 64 位操作系统，但具有特定要求和限制。可以在与 vCenter Server 相同的物理机或虚拟机或者一个单独的服务器上安装 View Composer。

表 1-3. View Composer 支持的操作系统

操作系统	版本	功能版本
Windows Server 2008 R2 SP1	64 位	Standard Enterprise Datacenter
Windows Server 2012 R2	64 位	Standard Datacenter
Windows Server 2016	64 位	Standard Datacenter

注 不再支持无 Service Pack 的 Windows Server 2008 R2。

如果要在 vCenter Server 以外的其他物理机或虚拟机上安装 View Composer，请参阅独立 View Composer 的硬件要求。

独立 View Composer 的硬件要求

如果通过用于 vCenter Server 的物理机或虚拟机将 View Composer 安装在其他物理机或虚拟机上，则必须使用可满足特定硬件要求的专用计算机。

独立的 View Composer 安装适用于在单独的 Windows Server 计算机上安装的 vCenter Server 或适用于基于 Linux 的 vCenter Server Appliance。VMware 建议在每个 View Composer 服务和 vCenter Server 实例之间建立一对一的映射关系。

表 1-4. View Composer 的硬件要求

硬件组件	需要	建议
处理器	1.4 GHz 或更快的 Intel 64 或 AMD 64 处理器，2 个 CPU	2GHz 或更快，4 个 CPU
网络连接	一个或多个 10/100 Mbps 网络接口卡 (NIC)	1 Gbps 网卡
内存	4GB RAM 或更高	对于包含 50 个或更多远程桌面的部署，至少需要 8 GB RAM
磁盘空间	40GB	60GB

重要 托管 View Composer 的物理机或虚拟机必须具有不会发生更改的 IP 地址。在 IPv4 环境中，配置静态 IP 地址。在 IPv6 环境中，计算机会自动获取不会发生更改的 IP 地址。

View Composer 和事件数据库的数据库要求

View Composer 需要使用 SQL 数据库来存储数据。View Composer 数据库必须位于 View Composer server 主机上，或者能够供其使用。（可选）您可以设置事件数据库以记录来自 Horizon Connection Server 的有关 Horizon 事件的信息。

如果已存在适用于 vCenter Server 的数据库服务器实例，且它的版本是位于 http://www.vmware.com/resources/compatibility/sim/interop_matrix.php 的“VMware 产品互操作性列表”中所列的版本，那么 View Composer 可以使用该现有实例。如果当前没有数据库服务器实例，则必须安装一个。

View Composer 支持 vCenter Server 所支持的部分数据库服务器。如果已将 vCenter Server 与 View Composer 不支持的数据库服务器结合使用，请继续将该数据库服务器用于 vCenter Server，然后另外安装一个单独的数据库服务器用于 View Composer。

重要 如果您在 vCenter Server 所在的 SQL Server 实例上创建 View Composer 数据库，请勿覆盖 vCenter Server 数据库。

有关受支持的数据库的最新信息，请参阅 http://www.vmware.com/resources/compatibility/sim/interop_matrix.php 上的“VMware 产品互操作性列表”。有关**解决方案/数据库互操作性**，选择产品和版本后，在“添加数据库”步骤中选择**任意**，然后单击**添加**可查看所有受支持的数据库的列表。

客户机操作系统的系统要求

2

运行 Horizon Agent 或 Horizon Persona Management 的系统必须满足特定的硬件和软件要求。

本章讨论了以下主题：

- Horizon Agent 支持的操作系统
- 独立 Horizon Persona Management 支持的操作系统
- 远程显示协议和软件支持

Horizon Agent 支持的操作系统

Horizon Agent 组件（在以前的版本中称为 View Agent）可帮助您实现会话管理、单点登录、设备重定向及其他功能。您必须在所有虚拟机、物理系统和 RDS 主机上安装 Horizon Agent。

受支持的客户机操作系统的类型和版本取决于 Windows 版本。有关受支持的 Windows 10 操作系统的列表的更新，请参阅 VMware 知识库 (KB) 文章 http://kb.vmware.com/kb/2149393。对于 Windows 10 以外的 Windows 操作系统，请参阅 VMware 知识库 (KB) 文章 http://kb.vmware.com/kb/2150295。

要查看安装 Horizon Agent 的 Windows 操作系统上支持的特定远程体验功能列表，请参阅 VMware 知识库 (KB) 文章 http://kb.vmware.com/kb/2150305。

要将 Horizon Persona Management 安装选项与 Horizon Agent 一起使用，您必须在 Windows 10、Windows 8、Windows 8.1、Windows 7、Windows Server 2012 R2、Windows Server 2008 R2 或 Windows Server 2016 虚拟机上安装 Horizon Agent。此选项不能在物理机或 RDS 主机上运行。

您可以在物理机上安装独立版 Horizon Persona Management。请参阅独立 Horizon Persona Management 支持的操作系统。

注 要使用 VMware Blast 显示协议，您必须在单会话虚拟机或 RDS 主机上安装 Horizon Agent。RDS 主机可以是物理机或虚拟机。VMware Blast 显示协议无法在单用户物理机上运行，但 Windows 10 RS4 企业版和更高版本除外。

为增强安全性，VMware 建议配置密码套件以消除已知漏洞。有关如何为运行 View Composer 或 Horizon Agent 的 Windows 计算机设置密码套件方面的域策略的说明，请参阅在 SSL/TLS 中禁用弱密码。

独立 Horizon Persona Management 支持的操作系统

独立 Horizon Persona Management 软件可以为未安装 Horizon Agent 的独立物理机和虚拟机提供用户配置管理功能。用户登录时，系统会从远程配置文件库将其配置文件动态下载至独立系统。

注　要为 Horizon 桌面配置用户配置管理，请安装带**用户配置管理**安装选项的 Horizon Agent。独立用户配置管理软件仅适用于非 Horizon 系统。

要查看独立 Horizon Persona Management 软件支持的操作系统列表，请参阅 VMware 知识库 (KB) 文章 http://kb.vmware.com/kb/2150295。

Microsoft 远程桌面服务不支持独立用户配置管理软件。

远程显示协议和软件支持

利用远程显示协议和软件可以访问远程桌面和应用程序。所用的远程显示协议取决于客户端设备的类型、您要连接远程桌面还是远程应用程序以及管理员如何配置桌面或应用程序池。

- PCoIP

  PCoIP (PC over IP) 针对已发布应用程序的交付或整个远程桌面环境为 LAN 或 WAN 中的广大用户提供了优化的桌面体验，包括应用程序、图像、音频和视频内容。PCoIP 可弥补因延迟增加或带宽减少导致的不便，确保最终用户在任何网络条件下均可保持高效。

- Microsoft RDP

  远程桌面协议实际上就是人们从家用计算机访问办公计算机时使用的多通道协议。Microsoft 远程桌面连接 (RDC) 使用 RDP 来传输数据。

- VMware Blast Extreme

  针对移动云优化的 VMware Blast Extreme 支持最广泛的启用 H.264 的客户端设备。在众多显示协议中，VMware Blast 具有最低的 CPU 消耗率，从而延长移动设备的电池寿命。VMware Blast Extreme 可对延迟的增加或带宽的减少进行补偿，并且还可同时利用 TCP 和 UDP 网络传输。

PCoIP

PCoIP (PC over IP) 针对已发布应用程序的交付或整个远程桌面环境为 LAN 或 WAN 中的广大用户提供了优化的桌面体验，包括应用程序、图像、音频和视频内容。PCoIP 可弥补因延迟增加或带宽减少导致的不便，确保最终用户在任何网络条件下均可保持高效。

PCoIP 显示协议可用于已发布的应用程序以及使用虚拟机、包含 Teradici 主机卡的物理机或 RDS 主机上的共享会话桌面的远程桌面。

PCoIP 功能

PCoIP 的主要功能包括：

- 企业防火墙范围以外的用户可将此协议与公司的虚拟专用网 (Virtual Private Network, VPN) 搭配使用，或者，用户也可通过安全、加密的方式连接到企业 DMZ 中的安全服务器或 Access Point 设备。

- 支持高级加密标准 (Advanced Encryption Standard, AES) 128 位加密，并且默认已启用。但是，您可以将加密密钥密码更改为 AES-256。
- 支持连接到装有 Horizon Agent 支持的操作系统中列出的 Horizon Agent 操作系统版本的 Windows 桌面。
- 从各种类型的客户端设备建立连接。
- 用于减少 LAN 和 WAN 的带宽使用的优化控制。
- 支持用 32 位色彩进行虚拟显示。
- 支持 ClearType 字体。
- 支持音频重定向，可针对 LAN 和 WAN 动态调整音频质量。
- 支持在某些客户端类型上使用网络摄像头和麦克风的实时音频-视频功能。
- 支持在客户端操作系统与远程桌面或已发布的应用程序之间复制和粘贴文本和图像（在部分客户端上受支持）。对于其他客户端类型，仅支持复制和粘贴纯文本。您无法在系统之间复制和粘贴系统对象，如文件夹和文件。
- 部分客户端类型支持多显示器。在某些客户端上，针对禁用 Aero 的 Windows 7 远程桌面，您最多可以使用 4 个分辨率最高为 2560 x 1600 的显示器或 3 个分辨率为 4K (3840 x 2160) 的显示器。此外还支持旋转显示和自动调整功能。

  启用 3D 功能时，支持最多 2 个分辨率最高为 1920 x 1200 的显示器或最多 1 个分辨率为 4K (3840 x 2160) 的显示器。
- 部分客户端类型支持 USB 重定向。
- 部分 Windows 客户端操作系统和部分远程桌面操作系统（安装了 Horizon Agent）支持 MMR 重定向。

有关哪些桌面操作系统支持特定 PCoIP 功能的信息，请参阅《Horizon 7 架构规划指南》文档。

有关哪些客户端设备支持特定 PCoIP 功能的信息，请访问 https://docs.vmware.com/cn/VMware-Horizon-Client/index.html。

建议的客户机操作系统设置

要以高分辨率全屏模式播放 720p 或更高格式的视频，推荐使用 1 GB 或以上的 RAM 及双 CPU。要对图形密集型应用程序（例如 CAD 应用程序）使用虚拟专用图形加速，建议使用 4GB RAM。

视频质量要求

480p 格式视频	当远程桌面使用单个虚拟 CPU 时，您可以在原始分辨率下播放 480p 或更低格式的视频。如果您希望以高清 Flash 或全屏模式播放视频，此桌面将需要使用双虚拟 CPU。即便使用双虚拟 CPU 桌面，以全屏模式播放 360p 这类格式较低的视频时也会出现落后于音频的情况，特别是在 Windows 客户端上。
720p 格式视频	当远程桌面具有双核虚拟 CPU 时，您可以在原始分辨率下播放 720p 格式的视频。如果您以高清或全屏模式播放 720p 视频，播放性能可能会受到影响。

1080p 格式视频	如果远程桌面使用双虚拟 CPU，您就可以播放 1080p 格式的视频，尽管可能需要将媒体播放器的窗口调小。
3D 呈现	可以将远程桌面配置为使用软件或硬件加速图形功能。这种软件加速图形功能使您能够运行 DirectX 9 和 OpenGL 2.1 应用程序，无需使用物理图形处理单元 (GPU)。这种硬件加速图形功能使虚拟机能够共享 vSphere 主机上的物理 GPU（图形处理单元），或者使物理 GPU 专用于单个虚拟机桌面。 对于 3D 应用程序，最多支持 2 台显示器，其屏幕分辨率最高为 1920 x 1200。远程桌面上的客户机操作系统必须是 Windows 7 或更高版本。

客户端系统的硬件要求

有关处理器和内存要求的信息，请参阅特定桌面或移动客户端设备类型的“使用 VMware Horizon Client”文档。请访问 https://docs.vmware.com/cn/VMware-Horizon-Client/index.html。

Microsoft RDP

远程桌面协议实际上就是人们从家用计算机访问办公计算机时使用的多通道协议。Microsoft 远程桌面连接 (RDC) 使用 RDP 来传输数据。

Microsoft RDP 是远程桌面所支持的显示协议，其使用虚拟机、物理机或 RDS 主机上的共享会话桌面。（已发布的应用程序仅支持 PCoIP 显示协议和 VMware Blast 显示协议。）Microsoft RDP 具有以下功能：

- RDP 7 真正实现了多显示器支持，最多可支持 16 个显示器。
- 您可以在本地系统与远程桌面之间复制和粘贴文本和系统对象（如文件夹和文件）。
- 支持用 32 位色彩进行虚拟显示。
- RDP 支持 128 位加密。
- 企业防火墙范围以外的用户可搭配使用此协议与公司的虚拟专用网 (VPN)，同时，用户也可通过安全、加密的方式连接到企业 DMZ 中的 View 安全服务器。

要支持到 Windows 7 和 Windows Server 2008 R2 的 TLSv1.1 和 TLSv1.2 连接，您必须应用 Microsoft 修补程序 KB3080079。

客户端系统的硬件要求

有关处理器和内存要求的信息，请参阅“使用 VMware Horizon Client”文档，以了解特定类型的客户端系统。请访问 https://docs.vmware.com/cn/VMware-Horizon-Client/index.html。

注　移动客户端 3.x 设备仅使用 PCoIP 显示协议。移动客户端 4.x 客户端仅使用 PCoIP 显示协议或 VMware Blast 显示协议。

VMware Blast Extreme

针对移动云优化的 VMware Blast Extreme 支持最广泛的启用 H.264 的客户端设备。在众多显示协议中，VMware Blast 具有最低的 CPU 消耗率，从而延长移动设备的电池寿命。VMware Blast Extreme 可对延迟的增加或带宽的减少进行补偿，并且还可同时利用 TCP 和 UDP 网络传输。

VMware Blast 显示协议可用于已发布的应用程序，以及使用 RDS 主机上的虚拟机或共享会话桌面的远程桌面。RDS 主机可以是物理机或虚拟机。VMware Blast 显示协议无法在单用户物理机上运行，但 Windows 10 RS4 企业版和更高版本除外。

注 运行 Windows 10 RS4 的物理计算机不支持“电影和电视”应用程序。

VMware Blast Extreme 功能

VMware Blast Extreme 的主要功能包括：

- 企业防火墙范围以外的用户可将此协议与企业的虚拟专用网 (Virtual Private Network, VPN) 搭配使用，或者，用户也可通过安全、加密的方式连接到企业 DMZ 中的安全服务器或 Access Point 设备。
- 支持高级加密标准 (Advanced Encryption Standard, AES) 128 位加密，并且默认已启用。但是，您可以将加密密钥密码更改为 AES-256。
- 支持连接到装有 Horizon Agent 支持的操作系统中列出的 Horizon Agent 操作系统版本的 Windows 桌面。
- 从各种类型的客户端设备建立连接。
- 用于减少 LAN 和 WAN 的带宽使用的优化控制。
- 在 Windows 代理中，使用 PerfMon 显示以下各项内容的性能计数器，这些计数器准确地显示系统的当前状态，系统也会以恒定的速率更新：
  - Blast 会话
  - 图像处理
  - 音频
  - CDR
  - USB：如果将 USB 流量配置为使用 VMware 虚拟通道 (VMware Virtual Channel, VVC)，则在 Windows 代理上使用 PerfMon 显示的 USB 计数器将有效。
  - Skype for Business：计数器仅用于控制流量。
  - 剪贴板
  - RTAV
  - 串行端口和扫描仪重定向功能
  - 虚拟打印
  - HTML5 MMR

    - Windows Media MMR：仅当将此功能配置为使用 VMware 虚拟通道 (VVC) 时，才会显示这些性能计数器。
- 在 Windows 客户端上出现短暂网络丢失期间保持网络连续性。
- 支持用 32 位色彩进行虚拟显示。
- 支持 ClearType 字体。
- 支持音频重定向，可针对 LAN 和 WAN 动态调整音频质量。
- 支持在某些客户端类型上使用网络摄像头和麦克风的实时音频-视频功能。
- 支持在客户端操作系统与远程桌面或已发布的应用程序之间复制和粘贴文本和图像（在部分客户端上受支持）。对于其他客户端类型，仅支持复制和粘贴纯文本。您无法在系统之间复制和粘贴系统对象，如文件夹和文件。
- 部分客户端类型支持多显示器。在某些客户端上，针对禁用 Aero 的 Windows 7 远程桌面，您最多可以使用 4 个分辨率最高为 2560 x 1600 的显示器或 3 个分辨率为 4K (3840 x 2160) 的显示器。此外还支持旋转显示和自动调整功能。

  启用 3D 功能时，支持最多 2 个分辨率最高为 1920 x 1200 的显示器或最多 1 个分辨率为 4K (3840 x 2160) 的显示器。
- 部分客户端类型支持 USB 重定向。
- 部分 Windows 客户端操作系统和部分远程桌面操作系统（安装了 Horizon Agent）支持 MMR 重定向。
- NVIDIA 显卡支持连接到未接显示器的物理机。为获得最佳性能，请使用支持 H.264 编码的显卡。

  如果同时安装附加分离式 GPU 和嵌入式 GPU，操作系统可能默认使用嵌入式 GPU。要修复此问题，您可以在设备管理器中禁用或移除设备。如果问题仍然存在，您可以安装嵌入式 GPU 的 WDDM 图形驱动程序，或在系统 BIOS 中禁用嵌入式 GPU。有关如何禁用嵌入式 GPU 的说明，请参阅系统文档。

小心　禁用嵌入式 GPU 可能导致以后无法访问相关功能，例如通过控制台访问 BIOS 设置或 NT 启动加载程序。

有关哪些客户端设备支持特定 VMware Blast Extreme 功能的信息，请访问 https://docs.vmware.com/cn/VMware-Horizon-Client/index.html。

LAN 唤醒

使用 Windows 10 RS4 企业版和更高版本的物理机支持 LAN 唤醒。使用此功能，用户可以在通过 Horizon Connection Server 连接时唤醒物理机。LAN 唤醒功能具有以下必备条件：

- 仅 IPv4 环境支持 LAN 唤醒 (Wake-on-LAN, WoL)。
- 当在 BIOS 设置及网卡设置中启用 LAN 唤醒后，必须将物理机配置为在接收 LAN 唤醒数据包时醒来。
- 将目标端口 9 用于接收来自连接服务器的 WoL 数据包。
- WoL 数据包是 IP 定向广播数据包，此类数据包在从 Horizon Connection Server 发送后必须能够到达 Horizon Agent。LAN 唤醒功能可在以下场景中使用：
    - 连接服务器和物理机上的 Horizon Agent 位于 LAN 环境的同一子网中。

- 连接服务器和 Horizon Agent 之间的所有路由器均已进行配置，允许到达要唤醒物理机所在的目标子网的 IP 定向广播数据包。

注 LAN 唤醒功能不支持物理 Windows 10 代理的浮动分配池。仅将 WoL 数据包发送到授权给特定用户的专用分配池。

建议的客户机操作系统设置

要以高分辨率全屏模式播放 720p 或更高格式的视频，推荐使用 1 GB 或以上的 RAM 及双 CPU。要对图形密集型应用程序（例如 CAD 应用程序）使用虚拟专用图形加速，建议使用 4GB RAM。

视频质量要求

480p 格式视频	当远程桌面使用单个虚拟 CPU 时，您可以在原始分辨率下播放 480p 或更低格式的视频。如果您希望以高清 Flash 或全屏模式播放视频，此桌面将需要使用双虚拟 CPU。即便使用双虚拟 CPU 桌面，以全屏模式播放 360p 这类格式较低的视频时也会出现落后于音频的情况，特别是在 Windows 客户端上。
720p 格式视频	当远程桌面具有双核虚拟 CPU 时，您可以在原始分辨率下播放 720p 格式的视频。如果您以高清或全屏模式播放 720p 视频，播放性能可能会受到影响。
1080p 格式视频	如果远程桌面使用双虚拟 CPU，您就可以播放 1080p 格式的视频，尽管可能需要将媒体播放器的窗口调小。
3D 呈现	可以将远程桌面配置为使用软件或硬件加速图形功能。这种软件加速图形功能使您能够运行 DirectX 9 和 OpenGL 2.1 应用程序，无需使用物理图形处理单元 (GPU)。这种硬件加速图形功能使虚拟机能够共享 vSphere 主机上的物理 GPU（图形处理单元），或者使物理 GPU 专用于单个虚拟桌面。 对于 3D 应用程序，最多支持 2 台显示器，最高屏幕分辨率为 1920 x 1200。远程桌面上的客户机操作系统必须为 Windows 7 或更高版本。

客户端系统的硬件要求

有关特定类型桌面或移动客户端设备的处理器和内容要求信息，请转到 https://docs.vmware.com/cn/VMware-Horizon-Client/index.html。

在 IPv6 环境中安装 Horizon 7

3

Horizon 7 支持使用 IPv6 替代 IPv4。您的环境必须为纯 IPv6 或纯 IPv4 环境。Horizon 7 不支持 IPv6 和 IPv4 混合的环境。

IPv4 环境中支持的所有 Horizon 7 功能并非在 IPv6 环境中均受支持。Horizon 7 不支持从 IPv4 环境升级到 IPv6 环境。另外，Horizon 7 不支持在 IPv4 和 IPv6 环境之间迁移。

重要 要在 IPv6 环境中运行 Horizon 7，安装所有 Horizon 7 组件时必须指定 IPv6。

本章讨论了以下主题：

- 在 IPv6 环境中设置 Horizon 7
- IPv6 环境中支持的 vSphere 数据库和 Active Directory 版本
- IPv6 环境中 Horizon 7 Server 支持的操作系统
- IPv6 环境中桌面和 RDS 主机支持的 Windows 操作系统
- IPv6 环境中支持的客户端
- IPv6 环境中支持的远程协议
- IPv6 环境中支持的身份验证类型
- IPv6 环境中其他受支持的功能

在 IPv6 环境中设置 Horizon 7

要在 IPv6 环境中运行 Horizon 7，必须了解执行某些管理任务时特定于 IPv6 的要求和选项。

安装 Horizon 7 前，必须有一个可以正常工作的 IPv6 环境。以下 Horizon 7 管理任务具有特定于 IPv6 的选项。

- 安装 Horizon 连接服务器。请参阅使用新配置安装 Horizon 连接服务器。
- 安装 View 副本服务器。请参阅安装 Horizon 连接服务器副本实例。
- 安装 View 安全服务器。请参阅安装安全服务器。
- 配置 PCoIP 外部 URL。请参阅为安全网关和安全加密链路连接配置外部 URL。
- 设置 PCoIP 外部 URL。请参阅设置连接服务器实例的外部 URL。
- 修改 PCoIP 外部 URL。请参阅设置连接服务器实例的外部 URL。

- 安装 Horizon Agent。请参阅设置桌面和应用程序池文档中的 Horizon Agent 安装主题。
- 安装 Horizon Client。请参阅 IPv6 环境中支持的客户端。

注 Horizon 7 不要求您在任何管理任务中输入 IPv6 地址。如果您可以指定完全限定域名 (FQDN) 或 IPv6 地址，强烈建议您指定 FQDN 以免出现潜在错误。

IPv6 环境中支持的 vSphere 数据库和 Active Directory 版本

在 IPv6 环境中，Horizon 7 支持特定的 vSphere、数据库服务器和 Active Directory 版本。

在 IPv6 环境中，支持以下 vSphere 版本。

- 6.7
- 6.5 U2
- 6.5
- 6.0
- 5.5 U2

在 IPv6 环境中，支持以下数据库服务器。

数据库服务器	版本	功能版本
SQL Server 2012 SP3	32/64 位	Standard、Enterprise
SQL Server 2012 SP4	32/64 位	Standard、Enterprise
SQL Server 2012 Express	32/64 位	可用空间
SQL Server 2014 AlwaysOn	32/64 位	Standard、Enterprise
SQL Server 2014 SP2	32/64 位	Standard、Enterprise
SQL Server 2016	64 位	Standard、Enterprise、Express
SQL Server 2016 AlwaysOn	64 位	Standard、Enterprise、Express
SQL Server 2017	64 位	Standard、Enterprise、Express、Developer
Oracle 11g R2	32/64 位	Standard、Standard Edition One、Enterprise
Oracle 12c R2	32/64 位	Standard、Standard Edition One、Enterprise

在 IPv6 环境中，支持以下 Active Directory 版本。

- Microsoft Active Directory 2008 R2
- Microsoft Active Directory 2012 R2

IPv6 环境中 Horizon 7 Server 支持的操作系统

在 IPv6 环境中，必须在特定的 Windows Server 操作系统中安装 Horizon 7 Server。

Horizon 7 Server 包括连接服务器实例、副本服务器、安全服务器和 Horizon 7 Composer 实例。

操作系统	功能版本
Windows Server 2016	Standard、Enterprise
Windows Server 2008 R2 SP1	Standard、Enterprise
Windows Server 2012 R2	Standard

IPv6 环境中桌面和 RDS 主机支持的 Windows 操作系统

在 IPv6 环境中，Horizon 7 支持桌面计算机和 RDS 主机使用特定的 Windows 操作系统。RDS 主机向用户提供基于会话的桌面和应用程序。

受支持的客户机操作系统的类型和版本取决于 Windows 版本。有关受支持的 Windows 10 操作系统的列表的更新，请参阅 VMware 知识库 (KB) 文章 http://kb.vmware.com/kb/2149393。对于 Windows 10 以外的 Windows 操作系统，请参阅 VMware 知识库 (KB) 文章 http://kb.vmware.com/kb/2150295。

要查看安装 Horizon Agent 的 Windows 操作系统上支持的特定远程体验功能列表，请参阅 VMware 知识库 (KB) 文章 http://kb.vmware.com/kb/2150305。

IPv6 环境中支持的客户端

在 IPv6 环境中，Horizon 7 支持在特定桌面操作系统中运行的客户端。

表 3-1. 支持的 Windows 操作系统

操作系统	版本	功能版本
Windows 7 和 Windows 7 SP1	32 位或 64 位	Home、Enterprise、Professional 和 Ultimate
Windows 8 和 Windows 8.1	32 位或 64 位	Pro、Enterprise 和 Industry Embedded
Windows 10	32 位或 64 位	Home、Pro、Pro for Workstations、Enterprise 和 IoT Enterprise

对于 iOS 设备，支持在 iOS 9.2 或更高版本中运行的 Horizon Client 4.1 或更高版本。

对于 Android 和 macOS 设备，需要使用 Horizon Client 4.9 或更高版本。

不支持以下类型的客户端。

- 在 Linux、Chrome OS、Windows 10 UWP 或 Windows 应用商店上运行的客户端
- iOS 9.1 或更低版本
- PCoIP 零客户端

IPv6 环境中支持的远程协议

在 IPv6 环境中，Horizon 7 支持特定的远程协议。

支持以下远程协议：

- RDP
- 包含安全加密链路的 RDP

- PCoIP
- 通过 PCoIP 安全网关的 PCoIP
- VMware Blast
- 通过 Blast 安全网关的 VMware Blast
- Blast Extreme 自适应传输 (Blast Extreme Adaptive Transport, BEAT)

IPv6 环境中支持的身份验证类型

在 IPv6 环境中，Horizon 7 支持特定的身份验证类型。

支持以下身份验证类型：

- 使用 Active Directory 的密码身份验证
- 智能卡
- 单点登录

不支持以下身份验证类型：

- SecurID
- RADIUS
- SAML

IPv6 环境中其他受支持的功能

在 IPv6 环境中，Horizon 7 支持前述主题中未涵盖的某些功能。

支持以下功能：

- 应用程序池
- 音频输出
- 完整虚拟机或 Horizon 7 Composer 链接克隆的自动桌面池

  注 不支持即时克隆的自动桌面池。

- Blast Extreme 自适应传输 (BEAT)
- 客户体验提升计划 (CEIP)
- 磁盘空间回收
- 事件
- HTML5 多媒体重定向
- LDAP 备份
- 手动桌面池，包括 vCenter Server 虚拟机、物理机以及不受 vCenter Server 管理的虚拟机
- 本地 NFS 快照 (VAAI)

- Horizon 性能跟踪器
- 用户配置管理
- 实时音频-视频 (RTAV)
- RDS 桌面池
- RDS 主机 3D
- 基于角色的管理
- 会话协作
- 单点登录，包括以当前用户身份登录功能
- 系统运行状况控制板
- ThinApp
- Unity Touch
- USB 重定向
- Horizon 7 Composer Agent
- Horizon 7 Storage Accelerator
- Horizon 7 Composer 数据库备份
- 虚拟打印
- VMware 音频
- VMware 视频
- 适用于 Skype for Business 的 VMware Virtualization Pack（仅限 Windows）

不支持以下功能：

- 客户端驱动器重定向
- 客户端 IP 透明度（仅限 64 位）
- Cloud Pod 架构
- 设备桥接
- 文件关联
- Flash URL 重定向
- HTML Access
- Log Insight
- Lync
- 扫描仪重定向
- 串行端口重定向

- Syslog
- Teradici TERA 主机卡
- TSMMR
- URL 重定向
- vSAN
- 虚拟卷
- vRealize Operations Desktop Agent

以 FIPS 模式安装 Horizon 7

4

Horizon 7 可以使用 FIPS（联合信息处理标准）140-2 兼容算法来执行加密操作。您可以通过以 FIPS 模式安装 Horizon 7 来启用这些算法。

在 FIPS 模式下，并非所有 Horizon 7 功能都受支持。此外，Horizon 7 不支持从非 FIPS 安装升级到 FIPS 安装。

注 为确保 Horizon 7 以 FIPS 模式运行，必须在安装所有 Horizon 7 组件时启用 FIPS。

本章讨论了以下主题：

- 以 FIPS 模式安装 Horizon 7 的概述
- FIPS 模式的系统要求

以 FIPS 模式安装 Horizon 7 的概述

要以 FIPS 模式安装 Horizon 7，必须先在 Windows 环境中启用 FIPS 模式。然后，以 FIPS 模式安装所有 Horizon 7 组件。

仅当在 Windows 环境中启用了 FIPS 模式时，以 FIPS 模式安装 Horizon 7 的选项才可用。有关在 Windows 中启用 FIPS 模式的更多信息，请访问 https://support.microsoft.com/en-us/kb/811833。

注 Horizon Administrator 不会指示是否正在 FIPS 模式下运行 Horizon 7。

要以 FIPS 模式安装 Horizon 7，请执行以下管理任务。

- 安装连接服务器时，请选择 FIPS 模式选项。请参阅使用新配置安装 Horizon 连接服务器。
- 安装副本服务器时，请选择 FIPS 模式选项。请参阅安装 Horizon 连接服务器副本实例。
- 在安装安全服务器之前，请在 Horizon Administrator 中取消选择全局设置**使用 IPSec 进行安全服务器连接**，并手动配置 IPsec。请参阅 http://kb.vmware.com/kb/2000175。
- 安装安全服务器时，请选择 FIPS 模式选项。请参阅安装安全服务器。
- 当 Windows 系统配置为使用 FIPS 操作，而 Horizon 7 配置为通过 IPSec 在连接服务器和安全服务器之间通信时，安全服务器安装会失败。在 IPv4 环境中，指定 PCoIP 外部 URL 作为 IP 地址，端口号为 4172。在 IPv6 环境中，可以指定 IP 地址或完全限定域名，端口号为 4172。在两种环境中，都不要包含协议名称。

  例如，在 IPv4 环境中：`10.20.30.40:4172`

客户端必须能够使用 URL 访问安全服务器。

- 为 View Composer 和 Horizon Agent 计算机禁用弱密码。请参阅在 SSL/TLS 中禁用弱密码。
- 安装 View Composer 时，请选择 FIPS 模式选项。请参阅第 6 章，安装 View Composer。
- 安装 Horizon Agent 时，请选择 FIPS 模式选项。请参阅《在 Horizon 7 中设置虚拟桌面》或《在 Horizon 7 中设置已发布的桌面和应用程序》文档中的 Horizon Agent 安装主题。
- 对于 Windows 客户端，请在客户端操作系统中启用 FIPS 模式，并在安装适用于 Windows 的 Horizon Client 时选择 FIPS 模式选项。请参阅《适用于 Windows 的 VMware Horizon Client 安装和设置指南》文档。
- 对于 Linux 客户端，请在客户端操作系统中启用 FIPS 模式。请参阅《适用于 Linux 的 VMware Horizon Client 安装和设置指南》文档。

FIPS 模式的系统要求

要支持 FIPS 模式，您的 Horizon 7 部署必须满足以下要求。

vSphere	■ vCenter Server 6.0 或更高版本 ■ ESXi 6.0 或更高版本
远程桌面	■ 任何具有 FIPS 证书的 Windows 平台。有关信息，请参阅 Microsoft TechNet 网站上的“FIPS 140 验证”。 ■ View Agent 6.2 或更高版本或者 Horizon Agent 7.0 或更高版本，仅限 Windows 平台
Horizon Client	■ 任何具有 FIPS 证书的 Windows 平台。有关信息，请参阅 Microsoft TechNet 网站上的“FIPS 140 验证”。 ■ 适用于 Windows 的 Horizon Client 3.5 或更高版本
加密协议	■ TLSv1.2

准备 Active Directory

5

Horizon 7 可利用您现有的 Microsoft Active Directory 基础架构对用户进行身份验证和管理。您必须执行特定的任务来准备 Active Directory，以便将其与 Horizon 7 一起使用。

Horizon 7 支持以下 Active Directory 域服务 (AD DS) 域功能级别：

- Windows Server 2008
- Windows Server 2008 R2
- Windows Server 2012
- Windows Server 2012 R2
- Windows Server 2016

本章讨论了以下主题：

- 配置域和信任关系
- 为远程桌面创建 OU
- 为 Kiosk 模式客户端帐户创建组织单位和组
- 创建用户组
- 为 vCenter Server 创建用户帐户
- 为独立的 View Composer Server 创建用户帐户
- 为 View Composer AD 操作创建用户帐户
- 为即时克隆操作创建用户帐户
- 配置受限制的组策略
- 使用 Horizon 7 组策略管理模板文件
- 为智能卡身份验证准备 Active Directory
- 在 SSL/TLS 中禁用弱密码

配置域和信任关系

您必须将每个连接服务器主机加入到 Active Directory 域。主机不能是域控制器。

Active Directory 还会管理 Horizon Agent 计算机（包括单用户计算机和 RDS 主机），以及 Horizon 7 部署中的用户和组。您可以授权用户和组访问远程桌面和应用程序，以及在 Horizon Administrator 中选择用户和组以作为管理员。

您可以将 Horizon Agent 计算机、View Composer Server，以及用户和组置于以下 Active Directory 域中：

- 连接服务器域
- 与连接服务器域之间具有双向信任关系的其他域
- 与连接服务器域位于不同的林中且与连接服务器域之间存在单向外部或领域信任关系的域
- 与连接服务器域位于不同的林中且与连接服务器域之间存在单向或双向可传递林信任关系的域

将使用 Active Directory 针对连接服务器域以及与其存在信任协议的任何其他用户域对用户进行身份验证。

如果用户和组位于单向信任域中，您必须在 Horizon Administrator 中为管理员用户提供辅助凭据。管理员必须具有辅助凭据才能访问单向信任域。单向信任域可以是外部域，也可以是具有可传递林信任关系的域。

仅 Horizon Administrator 会话需要使用辅助凭据，最终用户的桌面或应用程序会话则不需要使用该凭据。仅管理员用户需要使用辅助凭据。

您可以使用 `vdmadmin -T` 命令提供辅助凭据。

- 您可以为各个管理员用户配置辅助凭据。
- 对于林信任关系，您可以为林根域配置辅助凭据。然后，连接服务器可以枚举具有林信任关系的子域。

有关更多信息，请参阅《Horizon 7 管理指南》文档中的“使用 -T 选项为管理员提供辅助凭据”。

单向受信任的域不支持对用户进行智能卡和 SAML 身份验证。

注　由于安全服务器不会访问包括 Active Directory 在内的任何身份验证存储库，因此，它们不需要位于 Active Directory 域中。

信任关系和域过滤

为确定可访问的域，连接服务器实例会从其自身所在的域开始遍历信任关系。

对于一小组连接良好的域，连接服务器能够快速确定完整的域列表，但随着域数量的不断增多或域之间连接性的逐渐降低，确定完整域列表所需的时间也会随之增加。另外，该列表还可能包含您不希望用户在连接到其远程桌面和应用程序时为其提供的域。

您可以使用 `vdmadmin` 命令来配置域过滤，以限制连接服务器实例搜索并向用户显示的域。有关更多信息，请参阅《Horizon 7 管理指南》文档。

如果为林信任关系配置了名称后缀排除，则使用配置的排除过滤林子域列表。除了使用 `vdmadmin` 命令指定的过滤以外，还会应用名称后缀排除过滤。

为远程桌面创建 OU

您应为远程桌面专门创建一个组织单位 (OU)。组织单位是对 Active Directory 的细分，包含用户、组、计算机或其他组织单位。

为避免组策略设置应用到桌面所在域中的其他 Windows 服务器或工作站，您可以为 Horizon 7 组策略创建一个 GPO，并将其链接到包含您的远程桌面的 OU。您也可以将组织单位的控制权委托给下级组，如服务器操作员或单独用户。

如果您使用的是 View Composer，则应为链接克隆桌面创建一个基于远程桌面 OU 的单独 Active Directory 容器。在 Active Directory 中具有 OU 管理员权限的管理员可以在不具备域管理员权限的情况下置备链接克隆桌面。如果您更改了 Active Directory 的管理员凭据，则必须更新 View Composer 中的凭据信息。

为 Kiosk 模式客户端帐户创建组织单位和组

Kiosk 模式的客户端是指运行客户端软件以连接到连接服务器实例并启动远程桌面会话的瘦客户端或锁定 PC。如果您在 Kiosk 模式中配置客户端，则应在 Active Directory 中为 Kiosk 模式客户端帐户创建专用组织单位和组。

为 Kiosk 模式的客户端帐户创建专用组织单位和组可使客户端系统免受意外侵袭并简化客户端配置和管理。

有关更多信息，请参阅《Horizon 7 管理指南》文档。

创建用户组

您应在 Active Directory 中为不同类型的用户创建组。例如，您可以为最终用户创建一个名为 Horizon 7 Users 的组，为将要管理远程桌面和应用程序的用户创建另一个名为 Horizon 7 Administrators 的组。

为 vCenter Server 创建用户帐户

您必须在 Active Directory 中创建一个用户帐户与 vCenter Server 一起使用。在 Horizon Administrator 中添加 vCenter Server 实例时，需要指定该用户帐户。

您必须为用户帐户授予在 vCenter Server 中执行特定操作的特权。可以创建拥有合适特权的 vCenter Server 角色，并将该角色分配给 vCenter Server 用户。您添加到 vCenter Server 角色的特权列表各不相同，具体取决于您是否通过 View Composer 使用 Horizon 7。请参阅为 vCenter Server、View Composer 和即时克隆配置用户帐户了解有关配置这些特权的信息。

如果 View Composer 与 vCenter Server 安装在同一计算机上，则必须将 vCenter Server 用户添加到 vCenter Server 计算机上的本地管理员组。此要求允许 Horizon 7 对 View Composer 服务进行身份验证。

如果 View Composer 与 vCenter Server 安装在不同计算机上，则无需将 vCenter Server 用户作为 vCenter Server 计算机上的本地管理员。但是，您必须创建独立的 View Composer Server 用户帐户，且该用户帐户必须是 View Composer 计算机上的本地管理员。

为独立的 View Composer Server 创建用户帐户

如果 View Composer 与 vCenter Server 安装在不同计算机上，您必须在 Active Directory 中创建一个域用户帐户，Horizon 7 可使用该用户帐户对独立计算机上的 View Composer 服务进行身份验证。

该用户帐户必须处于您的连接服务器主机所在的域中，或者处于受信任的域中。必须将该用户帐户添加到独立 View Composer 计算机上的本地管理员组中。

在 Horizon Administrator 中配置 View Composer 设置并选择**独立的 View Composer Server** 时，需要指定该用户帐户。请参阅配置 View Composer 设置。

为 View Composer AD 操作创建用户帐户

如果使用 View Composer，则必须在 Active Directory 中创建一个用户帐户，以允许 View Composer 在 Active Directory 中执行特定操作。View Composer 需要使用该帐户将链接克隆虚拟机加入到您的 Active Directory 域中。

为确保安全性，您应当创建一个单独的用户帐户，以供 View Composer 使用。通过创建单独的帐户，可以确保该帐户不具有针对其他目的定义的额外特权。您可以为该帐户授予在指定的 Active Directory 容器中创建和移除计算机对象所需的最低特权。例如，View Composer 帐户不需要域管理员特权。

步骤

1 在 Active Directory 中，在您的连接服务器主机所在的域或某个受信任的域中创建一个用户帐户。

2 在用于创建和接收链接克隆计算机帐户的 Active Directory 容器中，授予该帐户**创建计算机对象**、**删除计算机对象**和**写入全部属性**权限。

以下列表显示了该用户帐户需要的所有权限，包括默认分配的权限：

- 列出内容
- 读取全部属性
- 写入全部属性
- 读取权限
- 重置密码
- 创建计算机对象
- 删除计算机对象

注 如果为桌面池选择**允许重用预先存在的计算机帐户**设置，则所需的权限较少。确保已将以下权限分配给用户帐户：

- 列出内容
- 读取全部属性
- 读取权限
- 重置密码

3 确保该用户帐户的权限可应用于 Active Directory 容器及其所有子对象。

后续步骤

在 Horizon Administrator 中执行以下操作时指定该帐户：在“添加 vCenter Server”向导中配置 View Composer 域，以及配置和部署链接克隆桌面池。

为即时克隆操作创建用户帐户

在部署即时克隆之前，必须创建一个在 Active Directory 中拥有某些操作执行权限的用户帐户。

在部署即时克隆桌面池前添加即时克隆域管理员时，可选择此帐户。有关更多信息，请参阅《在 Horizon 7 中设置虚拟桌面》文档中的“添加即时克隆域管理员”。

步骤

1 在 Active Directory 中，在连接服务器所在的域或某个受信任的域中创建用户帐户。

2 在即时克隆计算机帐户所在的容器中，授予该帐户**创建计算机对象**、**删除计算机对象**和**写入全部属性**权限。

以下列表显示了该用户帐户需要的权限，包括默认分配的权限：

- 列出内容
- 读取全部属性
- 写入全部属性
- 读取权限
- 重置密码
- 创建计算机对象
- 删除计算机对象

确保这些权限应用于正确的容器及其所有子对象。

配置受限制的组策略

要连接到远程桌面，用户必须是远程桌面本地远程桌面用户组的成员。您可以使用 Active Directory 中“受限制的组”策略，将用户或组添加到每个远程桌面（已加入到域中）的本地远程桌面用户组中。

“受限制的组”策略会设置域中计算机的本地组成员关系，使之与“受限制的组”策略中定义的成员关系列表设置相匹配。远程桌面用户组的成员始终会添加到每个加入域的远程桌面的本地远程桌面用户组中。添加新用户时，您只需要将其添加到您的远程桌面用户组。

前提条件

在 Active Directory 中，为您的域中的远程桌面用户创建一个组。

步骤

1 在 Active Directory 服务器上，导航至组策略管理插件。

AD 版本	导航路径
Windows 2003	a 选择**开始 > 所有程序 > 管理工具 > Active Directory 用户和计算机**。 b 右键单击域，然后单击**属性**。 c 在**组策略**选项卡上，单击**打开**以打开组策略管理插件。 d 右键单击**默认域策略**并单击**编辑**。
Windows 2008	a 选择**开始 > 管理工具 > 组策略管理**。 b 展开您的域，右键单击**默认域策略**并单击**编辑**。
Windows 2012 R2	a 选择**开始 > 管理工具 > 组策略管理**。 b 展开您的域，右键单击**默认域策略**并单击**编辑**。
Windows 2016	a 选择**开始 > 管理工具 > 组策略管理**。 b 展开您的域，右键单击**默认域策略**并单击**编辑**。

2 展开**计算机配置**区域，然后打开 **Windows 设置\安全性设置**。

3 右键单击**受限制的组**，然后选择**添加组**以添加远程桌面用户组。

4 右键单击新的受限制远程桌面用户组，并将远程桌面用户组添加到组成员列表。

5 单击**确定**保存更改。

使用 Horizon 7 组策略管理模板文件

Horizon 7 中包含多个特定于组件的组策略管理 (ADMX) 模板文件。

为 Horizon 7 提供组策略设置的所有 ADMX 文件包含在 `VMware-Horizon-Extras-Bundle-x.x.x-yyyyyyy.zip` 中，其中 *x.x.x* 是版本，*yyyyyyy* 是内部版本号。您可以从 VMware 下载站点中下载该文件，网址为 https://my.vmware.com/web/vmware/downloads。在“桌面和最终用户计算”下，选择 VMware Horizon 7 下载，其中包含 ZIP 文件。

通过将这些文件中的策略设置添加到 Active Directory 中新的或现有 GPO，并将其链接到包含桌面的组织单位，您可以优化并保护远程桌面。

有关使用 Horizon 7 组策略设置的信息，请参阅《Horizon 7 管理指南》和《在 Horizon 7 中配置远程桌面功能》文档。

为智能卡身份验证准备 Active Directory

实施智能卡身份验证时，您可能需要在 Active Directory 中执行特定的任务。

- 为智能卡用户添加 UPN

  由于智能卡登录依赖用户主体名称 (UPN)，因此在 Horizon 7 中使用智能卡进行身份验证的用户和管理员的 Active Directory 帐户必须具备有效的 UPN。

- 将根证书添加到受信任的根证书颁发机构

  如果使用证书颁发机构 (CA) 颁发智能卡登录或域控制器证书，则必须将根证书添加到 Active Directory 中受信任的根证书颁发机构组策略中。如果 Windows 域控制器充当根 CA，则不需要执行此步骤。

- 将中间证书添加到中间证书颁发机构

  如果使用中间证书颁发机构 (CA) 颁发智能卡登录或域控制器证书，则必须将中间证书添加到 Active Directory 的中间证书颁发机构组策略中。

- 将根证书添加到 Enterprise NTAuth 存储

  如果使用 CA 颁发智能卡登录或域控制器证书，则必须将根证书添加到 Active Directory 中的 Enterprise NTAuth 存储。如果 Windows 域控制器充当根 CA，则不需要执行此步骤。

为智能卡用户添加 UPN

由于智能卡登录依赖用户主体名称 (UPN)，因此在 Horizon 7 中使用智能卡进行身份验证的用户和管理员的 Active Directory 帐户必须具备有效的 UPN。

如果智能卡用户所在的域和颁发根证书的域不同，您必须将用户的 UPN 设置为受信任 CA 的根证书内包含的使用者备用名称 (SAN)。如果您的根证书是从智能卡用户当前所在域中的服务器上颁发的，则不需要修改用户的 UPN。

注 即便是从同一个域颁发证书，您仍然可能需要设置内置 Active Directory 帐户的 UPN。内置帐户（包括 Administrator 帐户）在默认情况下未设置 UPN。

前提条件

- 通过查看证书属性，获取受信任 CA 的根证书中包含的 SAN。
- 如果您的 Active Directory 服务器上没有“ADSI 编辑”实用程序，请从 Microsoft 网站下载并安装相应的 Windows 支持工具。

步骤

1. 在 Active Directory 服务器上，启动“ADSI 编辑”实用程序。
2. 在左侧窗格中，展开用户所在的域并双击 `CN=Users`。
3. 在右侧窗格中，右键单击用户，然后单击**属性**。
4. 双击 `userPrincipalName` 属性并键入受信任 CA 证书的 SAN 值。
5. 单击**确定**保存属性设置。

将根证书添加到受信任的根证书颁发机构

如果使用证书颁发机构 (CA) 颁发智能卡登录或域控制器证书，则必须将根证书添加到 Active Directory 中受信任的根证书颁发机构组策略中。如果 Windows 域控制器充当根 CA，则不需要执行此步骤。

步骤

1 在 Active Directory 服务器上，导航至组策略管理插件。

AD 版本	导航路径
Windows 2003	a 选择**开始 > 所有程序 > 管理工具 > Active Directory 用户和计算机**。 b 右键单击域，然后单击**属性**。 c 在**组策略**选项卡上，单击**打开**以打开组策略管理插件。 d 右键单击**默认域策略**并单击**编辑**。
Windows 2008	a 选择**开始 > 管理工具 > 组策略管理**。 b 展开您的域，右键单击**默认域策略**并单击**编辑**。
Windows 2012 R2	a 选择**开始 > 管理工具 > 组策略管理**。 b 展开您的域，右键单击**默认域策略**并单击**编辑**。
Windows 2016	a 选择**开始 > 管理工具 > 组策略管理**。 b 展开您的域，右键单击**默认域策略**并单击**编辑**。

2 展开**计算机配置**区域，然后打开 **Windows 设置\安全性设置\公钥**。

3 右键单击**受信任的根证书颁发机构**，然后选择**导入**。

4 按照向导中的提示导入根证书（如 `rootCA.cer`）并单击**确定**。

5 关闭“组策略”窗口。

此时，域中的所有系统在其信任的根存储中都有一个根证书的副本。

后续步骤

如果中间证书颁发机构 (CA) 为您颁发了智能卡登录或域控制器证书，请将此中间证书添加到 Active Directory 中的中间证书颁发机构组策略中。请参阅将中间证书添加到中间证书颁发机构。

将中间证书添加到中间证书颁发机构

如果使用中间证书颁发机构 (CA) 颁发智能卡登录或域控制器证书，则必须将中间证书添加到 Active Directory 的中间证书颁发机构组策略中。

步骤

1 在 Active Directory 服务器上，导航至组策略管理插件。

AD 版本	导航路径
Windows 2003	a 选择**开始 > 所有程序 > 管理工具 > Active Directory 用户和计算机**。 b 右键单击域，然后单击**属性**。 c 在**组策略**选项卡上，单击**打开**以打开组策略管理插件。 d 右键单击**默认域策略**并单击**编辑**。
Windows 2008	a 选择**开始 > 管理工具 > 组策略管理**。 b 展开您的域，右键单击**默认域策略**并单击**编辑**。

AD 版本	导航路径
Windows 2012 R2	a 选择**开始 > 管理工具 > 组策略管理**。 b 展开您的域，右键单击**默认域策略**并单击**编辑**。
Windows 2016	a 选择**开始 > 管理工具 > 组策略管理**。 b 展开您的域，右键单击**默认域策略**并单击**编辑**。

2 展开**计算机配置**区域，然后打开 **Windows 设置\安全性设置\公钥**策略。

3 右键单击**中间证书颁发机构**，然后选择**导入**。

4 按照向导中的提示导入中间证书（如 `intermediateCA.cer`）并单击**确定**。

5 关闭“组策略”窗口。

此时，域中的所有系统在其中间证书颁发机构存储区中都有一个中间证书的副本。

将根证书添加到 Enterprise NTAuth 存储

如果使用 CA 颁发智能卡登录或域控制器证书，则必须将根证书添加到 Active Directory 中的 Enterprise NTAuth 存储。如果 Windows 域控制器充当根 CA，则不需要执行此步骤。

步骤

- 在 Active Directory 服务器上使用 `certutil` 命令，将证书发布到 Enterprise NTAuth 存储区中。

  例如：**`certutil –dspublish –f` *`CA 根证书路径`* `NTAuthCA`**

此时该 CA 即为颁发此类证书的受信任机构。

在 SSL/TLS 中禁用弱密码

为了提高安全性，您可以配置域策略 GPO（组策略对象），以确保 View Composer 和运行 View Agent 或 Horizon Agent 的基于 Windows 的计算机在使用 SSL/TLS 协议进行通信时不会使用弱密码。

步骤

1 在 Active Directory 服务器上编辑 GPO，方法是选择**开始 > 管理工具 > 组策略管理**，右键单击 GPO，然后选择**编辑**。

2 在组策略管理编辑器中，浏览到**计算机配置 > 策略 > 管理模板 > 网络 > SSL 配置设置**。

3 双击 **SSL 密码套件顺序**。

4 在“SSL 密码套件顺序”窗口中，单击**已启用**。

5 在“选项”窗格中，将“SSL 密码套件”文本框的全部内容替换为以下密码列表：

```
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256_P256,
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256_P384,
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA_P256,
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA_P384,
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA_P256,
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA_P384,
```

```
TLS_RSA_WITH_AES_128_CBC_SHA256,
TLS_RSA_WITH_AES_128_CBC_SHA,
TLS_RSA_WITH_AES_256_CBC_SHA256,
TLS_RSA_WITH_AES_256_CBC_SHA
```

为了便于查看，密码套件已分多行列在上方。将该列表粘贴到文本框中时，密码套件必须位于一行中，并且逗号后不含空格。

6 退出组策略管理编辑器。

7 重新启动 View Composer 和 View Agent 或 Horizon Agent 计算机以使新的组策略生效。

6 安装 View Composer

要使用 View Composer，您需要创建一个 View Composer 数据库、安装 View Composer 服务并优化您的 View 基础架构以支持 View Composer。您可以在安装 vCenter Server 的同一主机上或独立的主机上安装 View Composer 服务。

View Composer 是可选功能。如果您计划部署链接克隆桌面池，请安装 View Composer。

您必须通过许可来安装和使用 View Composer 功能。

注 在安装 View Composer 之前，请确认您已准备好 Active Directory。

本章讨论了以下主题：

- 准备 View Composer 数据库
- 为 View Composer 配置 SSL 证书
- 安装 View Composer 服务
- 对从 View Composer 进行的 vCenter 和 ESXi 连接启用 TLSv1.0
- 为 View Composer 配置基础架构

准备 View Composer 数据库

您必须创建一个数据库和数据源名 (Data Source Name, DSN) 来存储 View Composer 数据。

View Composer 服务中不包含数据库。如果您的网络环境中没有数据库实例，则必须安装一个。安装数据库实例后，需要将 View Composer 数据库添加到实例。

您可以将 View Composer 数据库添加到 vCenter Server 数据库所在的实例。您可以在本地或远程位置（连接网络的 Linux、UNIX 或 Windows Server 计算机）配置数据库。

View Composer 数据库存储有关 View Composer 所用连接和组件的信息：

- vCenter Server 连接
- Active Directory 连接
- View Composer 部署的链接克隆桌面
- View Composer 创建的副本

每个 View Composer 服务实例都必须有自己的 View Composer 数据库。多个 View Composer 服务不能共享一个 View Composer 数据库。

有关支持的数据库版本列表，请参阅 View Composer 和事件数据库的数据库要求。

要将 View Composer 数据库添加到已安装的数据库实例中，请选择下面一种操作过程。

- 为 View Composer 创建 SQL Server 数据库

  View Composer 可以将链接克隆桌面信息存储在 SQL Server 数据库中。您可以将数据库添加到现有 SQL Server 并为其配置 ODBC 数据源，从而创建一个 View Composer 数据库。

- 为 View Composer 创建 Oracle 数据库

  View Composer 可以将链接克隆桌面信息存储在 Oracle 12c 或 11g 数据库中。您可以将 View Composer 数据库添加到现有 Oracle 实例并为其配置 ODBC 数据源，从而创建一个 View Composer 数据库。您可以使用 Oracle 数据库配置助理或运行 SQL 语句来添加新的 View Composer 数据库。

为 View Composer 创建 SQL Server 数据库

View Composer 可以将链接克隆桌面信息存储在 SQL Server 数据库中。您可以将数据库添加到现有 SQL Server 并为其配置 ODBC 数据源，从而创建一个 View Composer 数据库。

步骤

1 将 View Composer 数据库添加到 SQL Server

  您可以向现有 Microsoft SQL Server 实例添加新的 View Composer 数据库，以存储 View Composer 的链接克隆数据。

2 （可选）通过手动创建数据库角色设置 SQL Server 数据库权限

  使用这一建议方法，View Composer 数据库管理员可以为 View Composer 管理员设置要通过 Microsoft SQL Server 数据库角色授予的权限。

3 将 ODBC 数据源添加到 SQL Server

  将 View Composer 数据库添加到 SQL Server 后，您必须配置一个指向新数据库的 ODBC 连接，以使该数据源能够向 View Composer 服务显示。

将 View Composer 数据库添加到 SQL Server

您可以向现有 Microsoft SQL Server 实例添加新的 View Composer 数据库，以存储 View Composer 的链接克隆数据。

如果该数据库位于将安装 View Composer 的系统本地，则您可以使用集成 Windows 身份验证（Integrated Windows Authentication）安全模式。如果数据库位于远程系统中，您将无法使用这种方式进行身份验证。

前提条件

- 确认已在将安装 View Composer 的计算机中或网络环境中安装了受支持的 SQL Server 版本。有关详细信息，请参阅 View Composer 和事件数据库的数据库要求。
- 确认使用 SQL Server Management Studio 创建和管理数据库。此外，还可以使用 SQL Server Management Studio Express，可从以下 Web 站点下载和安装该工具。

  http://www.microsoft.com/en-us/download/details.aspx?id=7593

步骤

1 在 View Composer 计算机中，选择**开始 > 所有程序 > Microsoft SQL Server 2014**、**Microsoft SQL Server 2012** 或 **Microsoft SQL Server 2008**。

2 选择 **SQL Server Management Studio**，然后连接到 SQL Server 实例。

3 在“对象浏览器”面板中，右键单击“数据库”条目并选择**新建数据库**。

对于数据库和日志文件，可以使用 `Initial size` 和 `Autogrowth` 参数的默认值。

4 在“新建数据库”对话框的“数据库名”文本框中键入一个名称。

例如：**`ViewComposer`**

5 单击**确定**。

SQL Server Management Studio 会将您的数据库添加到“对象浏览器”面板中的“数据库”条目中。

6 退出 Microsoft SQL Server Management Studio。

后续步骤

也可以按照（可选） 通过手动创建数据库角色设置 SQL Server 数据库权限中的说明操作

按照将 ODBC 数据源添加到 SQL Server 中的说明操作。

（可选） 通过手动创建数据库角色设置 SQL Server 数据库权限

使用这一建议方法，View Composer 数据库管理员可以为 View Composer 管理员设置要通过 Microsoft SQL Server 数据库角色授予的权限。

VMware 建议使用该方法，因为它不需要为安装和升级 View Composer 的 View Composer 管理员设置 **db_owner** 角色。

在此过程中，您可以提供自己的名称作为数据库登录名称、用户名和数据库角色。用户 **[vcmpuser]** 以及数据库角色 **VCMP_ADMIN_ROLE** 和 **VCMP_USER_ROLE** 均为示例名称。在创建 View Composer 数据库时会创建 **dbo** 架构。必须使用 **dbo** 架构名称。

前提条件

- 确认 View Composer 数据库已创建。请参阅将 View Composer 数据库添加到 SQL Server。

步骤

1 以 sysadmin (SA) 身份或使用具有 **sysadmin** 特权的用户帐户登录 Microsoft SQL Server Management Studio 会话。

2 创建一个将被授予 SQL Server 数据库权限的用户。

```
use ViewComposer
go
CREATE LOGIN [vcmpuser] WITH PASSWORD=N'vcmpuser!0', DEFAULT_DATABASE=ViewComposer,
DEFAULT_LANGUAGE=us_english, CHECK_POLICY=OFF
go
CREATE USER [vcmpuser] for LOGIN [vcmpuser]
```

```
go
use MSDB
go
CREATE USER [vcmpuser] for LOGIN [vcmpuser]
go
```

3 在 View Composer 数据库中，创建数据库角色 **VCMP_ADMIN_ROLE**。

4 在 View Composer 数据库中，向 **VCMP_ADMIN_ROLE** 授予特权。

   a 在 **dbo** 架构上，授予**更改**、**引用**和**插入**的架构权限。

   b 授予**创建表**、**创建视图**和**创建程序**的权限。

5 在 View Composer 数据库中，创建 **VCMP_USER_ROLE**。

6 在 View Composer 数据库中，在 **dbo** 架构上向 **VCMP_USER_ROLE** 授予**选择**、**插入**、**删除**、**更新**和**执行**的架构权限。

7 向用户 **[vcmpuser]** 授予 **VCMP_USER_ROLE**。

8 向用户 **[vcmpuser]** 授予 **VCMP_ADMIN_ROLE**。

9 在 MSDB 数据库中，创建数据库角色 **VCMP_ADMIN_ROLE**。

10 在 MSDB 中，向 **VCMP_ADMIN_ROLE** 授予特权。

   a 在 MSDB 表 `syscategories`、`sysjobsteps` 和 `sysjobs` 中，向用户 **[vcmpuser]** 授予**选择**权限。

   b 在 MSDB 存储过程 `sp_add_job`、`sp_delete_job`、`sp_add_jobstep`、`sp_update_job`、`sp_add_jobserver`、`sp_add_jobschedule` 和 `sp_add_category` 中，向角色 **VCMP_ADMIN_ROLE** 授予**执行**权限。

11 在 MSDB 数据库中，向用户 **[vcmpuser]** 授予 **VCMP_ADMIN_ROLE**。

12 使用 SQL Server 登录名 **vcmpuser** 创建 ODBC DSN。

13 安装 View Composer。

14 在 MSDB 数据库中，撤销用户 **[vcmpuser]** 的 **VCMP_ADMIN_ROLE** 角色。

   撤销该角色后，可以将该角色保留为非活动状态，也可以删除该角色以提高安全性。

有关创建 ODBC DSN 的说明，请参阅将 ODBC 数据源添加到 SQL Server。

有关安装 View Composer 的说明，请参阅安装 View Composer 服务。

将 ODBC 数据源添加到 SQL Server

将 View Composer 数据库添加到 SQL Server 后，您必须配置一个指向新数据库的 ODBC 连接，以使该数据源能够向 View Composer 服务显示。

为 View Composer 配置 ODBC DSN 时， 请确保针对您的环境建立适当级别的底层数据库连接。要获取保护数据库连接的相关信息，请参阅 SQL Server 文档。

如底层数据库连接使用 SSL 加密， 我们建议您使用由可信 CA 签发的 SSL 证书配置数据库服务器。如使用自签名证书，则您的数据库连接很可能 会受到中间人攻击。

前提条件

完成将 View Composer 数据库添加到 SQL Server 中介绍的步骤。

步骤

1 在将安装 View Composer 的计算机中，选择**开始 > 管理工具 > 数据源 (ODBC)**。

2 选择**系统 DSN** 选项卡。

3 单击**添加**，然后从列表中选择 **SQL 本地客户端**。

4 单击**完成**。

5 在**创建 SQL Server 的新数据源**设置向导中，键入 View Composer 数据库名和描述。

例如：**ViewComposer**

6 在“服务器”文本框中，键入 SQL Server 数据库名。

请使用 *host_name\server_name* 格式，其中 *host_name* 是计算机名，*server_name* 是 SQL Server 实例。

例如：**VCHOST1\VIM_SQLEXP**

7 单击**下一步**。

8 请确保已选中**连接到 SQL Server 以获得其他配置选项的默认设置**复选框，且选择了一个身份验证选项。

选项	描述
集成 Windows 身份验证	如果正在使用 SQL Server 本地实例，请选择该选项。该选项也被认为是受信任的身份验证。只有在本地计算机上运行 SQL Server 时才支持集成 Windows 身份验证。
SQL Server authentication（SQL Server 身份验证）	使用 SQL Server 的远程实例时请选择该选项。Windows NT 身份验证在远程 SQL Server 中不受支持。 如果手动设置 SQL Server 数据库权限并将其分配给用户，请对该用户进行身份验证。例如，对用户 **vcmpuser** 进行身份验证。如果未手动设置，则以 sysadmin (SA) 身份或使用具有 **sysadmin** 特权的用户帐户进行身份验证。

9 单击**下一步**。

10 选择**将默认数据库更改为**复选框并从列表中选择 View Composer 数据库的名称。

例如：**ViewComposer**

11 如 SQL Server 连接配置为启用 SSL， 则导航至 Microsoft SQL Server DSN 配置页面，然后选择**对数据使用强大的加密**。

12 完成并关闭 **Microsoft ODBC 数据源管理器**向导。

后续步骤

安装新的 View Composer 服务。请参阅安装 View Composer 服务。

为 View Composer 创建 Oracle 数据库

View Composer 可以将链接克隆桌面信息存储在 Oracle 12c 或 11g 数据库中。您可以将 View Composer 数据库添加到现有 Oracle 实例并为其配置 ODBC 数据源，从而创建一个 View Composer 数据库。您可以使用 Oracle 数据库配置助理或运行 SQL 语句来添加新的 View Composer 数据库。

- 将 View Composer 数据库添加到 Oracle 12c 或 11g

  可以使用 Oracle 数据库配置助理将新的 View Composer 数据库添加到现有 Oracle 12c 或 11g 实例。
- 使用 SQL 语句将 View Composer 数据库添加到 Oracle 实例
- 为 View Composer 配置 Oracle 数据库用户

  默认情况下，运行 View Composer 数据库的用户已拥有 Oracle 系统管理员权限。要限制运行 View Composer 数据库的用户的安全权限，必须为 Oracle 数据库用户配置特定的权限。
- 将 ODBC 数据源添加到 Oracle 12c 或 11g

  将 View Composer 数据库添加到 Oracle 12c 或 11g 实例后，必须配置一个指向新数据库的 ODBC 连接，以使该数据源对 View Composer 服务可见。

将 View Composer 数据库添加到 Oracle 12c 或 11g

可以使用 Oracle 数据库配置助理将新的 View Composer 数据库添加到现有 Oracle 12c 或 11g 实例。

前提条件

确认已在本地或远程计算机上安装了受支持的 Oracle 12c 或 11g 版本。请参阅 View Composer 和事件数据库的数据库要求。

步骤

1 在要添加 View Composer 数据库的计算机上启动**数据库配置助理**。

数据库版本	操作
Oracle 12c	选择**开始 > 所有程序 > Oracle-OraDb12c_home > 配置和迁移工具 > 数据库配置助理**。
Oracle 11g	选择**开始 > 所有程序 > Oracle-OraDb11g_home > 配置和迁移工具 > 数据库配置助理**。

2 在“操作”页面上，选择**创建数据库**。

3 在“数据库模板”页面上，选择**一般用途或事务处理**模板。

4 在“数据库标识”页面上，键入全局数据库名称和 Oracle 系统标识符 (System Identifier, SID) 前缀。

为简化起见，您可以为这两项使用相同的值。

5 在“管理选项”页面上，单击**下一步**接受默认设置。

6 在“数据库凭据”页面上，选择**为所有帐户使用相同管理密码**并键入密码。

7 在其余的配置页面上，均单击**下一步**接受默认设置。

8 在“创建选项”页面上，请验证是否已选中**创建数据库**选项并单击**完成**。

9 在“确认”页面中，查看选项并单击**确定**。

配置工具会创建数据库。

10 在“数据库创建完成”页面上，单击**确定**。

后续步骤

按照将 ODBC 数据源添加到 Oracle 12c 或 11g 中的说明操作。

使用 SQL 语句将 View Composer 数据库添加到 Oracle 实例

在创建数据库时，您可以自定义数据和日志文件的位置。

前提条件

View Composer 数据库必须拥有特定的表空间和特权。您可以使用 SQL 语句在 Oracle 12c 或 11g 数据库实例中创建 View Composer 数据库。

确认已在本地或远程计算机上安装了受支持的 Oracle 12c 或 11g 版本。有关详细信息，请参阅 View Composer 和事件数据库的数据库要求。

步骤

1 使用系统帐户登录到 SQL*Plus 会话。

2 执行以下 SQL 语句创建数据库。

```
CREATE SMALLFILE TABLESPACE "VCMP" DATAFILE '/u01/app/oracle/oradata/vcdb/vcmp01.dbf'
SIZE 512M AUTOEXTEND ON NEXT 10M MAXSIZE UNLIMITED LOGGING EXTENT MANAGEMENT LOCAL SEGMENT
SPACE MANAGEMENT AUTO;
```

在该示例中，VCMP 是 View Composer 数据库的示例名称，`vcmp01.dbf` 是数据库文件的名称。

在 Windows 环境中，请为 `vcmp01.dbf` 文件指定符合 Windows 规则的路径。

后续步骤

如果您希望用特定的安全权限运行 View Composer 数据库，请按照为 View Composer 配置 Oracle 数据库用户中的说明操作。

按照将 ODBC 数据源添加到 Oracle 12c 或 11g 中的说明操作

为 View Composer 配置 Oracle 数据库用户

默认情况下，运行 View Composer 数据库的用户已拥有 Oracle 系统管理员权限。要限制运行 View Composer 数据库的用户的安全权限，必须为 Oracle 数据库用户配置特定的权限。

前提条件

确认 View Composer 数据库是在 Oracle 12c 或 11g 实例中创建的。

步骤

1 使用系统帐户登录到 SQL*Plus 会话。

2 运行以下 SQL 命令创建具有适当权限的 View Composer 数据库用户。

```
CREATE USER "VCMPADMIN" PROFILE "DEFAULT" IDENTIFIED BY "oracle" DEFAULT TABLESPACE

"VCMP" ACCOUNT UNLOCK;
   grant connect to VCMPADMIN;
   grant resource to VCMPADMIN;
   grant create view to VCMPADMIN;
   grant create sequence to VCMPADMIN;
   grant create table to VCMPADMIN;
   grant create materialized view to VCMPADMIN;
   grant execute on dbms_lock to VCMPADMIN;
   grant execute on dbms_job to VCMPADMIN;
   grant unlimited tablespace to VCMPADMIN;
```

在此示例中，用户名为 VCMPADMIN，View Composer 数据库名称为 VCMP。

默认情况下，`resource` 角色已拥有 `create procedure`、`create table` 和 `create sequence` 特权。如果 `resource` 角色没有这些特权，请将其明确指定给 View Composer 数据库用户。

将 ODBC 数据源添加到 Oracle 12c 或 11g

将 View Composer 数据库添加到 Oracle 12c 或 11g 实例后，必须配置一个指向新数据库的 ODBC 连接，以使该数据源对 View Composer 服务可见。

为 View Composer 配置 ODBC DSN 时， 请确保针对您的环境建立适当级别的底层数据库连接。要获取保护数据库连接的信息，请参阅 Oracle 数据库文档。

如底层数据库连接使用 SSL 加密， 我们建议您使用由可信 CA 签发的 SSL 证书配置数据库服务器。如使用自签名证书，则您的数据库连接很可能 会受到中间人攻击。

前提条件

确认已完成将 View Composer 数据库添加到 Oracle 12c 或 11g 或使用 SQL 语句将 View Composer 数据库添加到 Oracle 实例中的步骤。

步骤

1 在 View Composer 数据库计算机中，选择**开始 > 管理工具 > 数据源 (ODBC)**。

2 从 **Microsoft ODBC 数据源管理器**向导中选择**系统 DSN** 选项卡。

3 单击**添加**，然后从列表中选择适当的 Oracle 驱动程序。

例如：**OraDb11g_home**

4 单击**完成**。

5 在“Oracle ODBC 驱动程序配置”对话框中，键入要用于 View Composer 的 DSN、对该数据源的描述以及用于连接数据库的用户 ID。

如果为 Oracle 数据库用户 ID 配置了特定的安全权限，就要指定该用户 ID。

注 安装 View Composer 服务时会使用 DSN。

6 从下拉菜单中选择“全局数据库名称”，指定 **TNS 服务名**。

Oracle 数据库配置助理会指定全局数据库名称。

7 要确认数据源，请单击**测试连接**，然后单击**确定**。

后续步骤

安装新的 View Composer 服务。请参阅安装 View Composer 服务。

为 View Composer 配置 SSL 证书

默认情况下，一个自签名证书会随 View Composer 一同安装。您可以使用默认证书进行测试，但对于生产用途来说，您应使用由证书颁发机构 (CA) 签发的证书替换默认证书。

您可以在安装 View Composer 之前或之后配置证书。在 View 5.1 和更高版本中，可以通过在已安装或要安装 View Composer 的 Windows Server 计算机上向 Windows 本地计算机证书存储区导入一个证书来配置证书。

- 如果在安装 View Composer 前导入由 CA 签发的证书，可以在安装 View Composer 时选择签名证书。这种方法避免了在安装后手动替换默认证书的步骤。
- 如果在安装 View Composer 后想使用新证书替换现有证书或默认的自签名证书，必须导入新证书并运行 `SviConfig ReplaceCertificate` 实用程序，以将新证书与 View Composer 使用的端口绑定。

有关配置 SSL 证书以及使用 `SviConfig ReplaceCertificate` 实用程序的详细信息，请参阅第 8 章，为 Horizon 7 Server 配置 TLS 证书。

如果您在同一 Windows Server 计算机上安装 vCenter Server 和 View Composer，它们可以使用相同的 SSL 证书，但必须单独为每个组件配置证书。

安装 View Composer 服务

要使用 View Composer，必须安装 View Composer 服务。Horizon 7 使用 View Composer 在 vCenter Server 中创建并部署链接克隆桌面。

您可以在安装 vCenter Server 的 Windows Server 计算机上安装 View Composer 服务，也可以在单独的 Windows Server 计算机上安装。独立安装的 View Composer 可以与 Windows Server 计算机上安装的 vCenter Server 以及基于 Linux 的 vCenter Server Appliance 协同工作。

View Composer 软件无法与任何其他 Horizon 7 软件组件（包括副本服务器、安全服务器、连接服务器、Horizon Agent 或 Horizon Client）共存于同一虚拟机或物理机上。

为增强安全性，我们建议配置密码套件以消除已知漏洞。有关如何为运行 View Composer 或 Horizon Agent 的 Windows 计算机设置密码套件方面的域策略的说明，请参阅在 SSL/TLS 中禁用弱密码。

前提条件

- 确认您的安装符合 View Composer 的要求中所述的 View Composer 要求。
- 确认要安装 View Composer 的计算机上未安装其他 Horizon 7 组件，包括连接服务器、安全服务器、Horizon Agent 或 Horizon Client。
- 确认您拥有安装和使用 View Composer 的许可。
- 确认您拥有在“ODBC 数据源管理器”向导中提供的 DSN、域管理员用户名和密码。安装 View Composer 服务时需要输入此信息。
- 如果希望在安装过程中为 View Composer 配置由 CA 签发的 SSL 证书，请确认您的证书已导入 Windows 本地计算机证书存储区。请参阅第 8 章，为 Horizon 7 Server 配置 TLS 证书。
- 确认 View Composer 计算机上运行的应用程序均未使用 Windows SSL 库，后者需要使用通过 Microsoft Secure Channel (Schannel) 安全软件包提供的 SSL 版本 2 (SSLv2)。View Composer 安装程序禁用了 Microsoft Schannel 上的 SSLv2。有些应用程序（例如，使用 Java SSL 的 Tomcat 和使用 OpenSSL 的 Apache）则不受此限制影响。
- 要运行 View Composer 安装程序，您必须是系统上具有管理员特权的用户。

步骤

1 从 VMware 产品页面 http://www.vmware.com/cn/products/ 将 View Composer 安装程序文件下载到 Windows Server 计算机。

安装程序文件名为 `VMware-viewcomposer-y.y.y-xxxxxx.exe`，其中，*xxxxxx* 为内部版本号，*y.y.y* 为版本号。此安装程序文件用于在 64 位 Windows Server 操作系统上安装 View Composer 服务。

2 要启动 View Composer 安装程序，请右键单击安装程序文件并选择**以管理员身份运行**。

3 接受 VMware 许可条款。

4 接受或更改目标文件夹。

5 键入在 Microsoft 或 Oracle **ODBC 数据源管理器**向导中提供的 View Composer 数据库的 DSN。

例如：**`VMware View Composer`**

> **注** 如果您没有为 View Composer 数据库配置 DSN，请单击 **ODBC DSN 设置**来配置一个名称。

6 键入您在 **ODBC 数据源管理器**向导中提供的域管理员用户名和密码。

如果为 Oracle 数据库用户配置了特定的安全权限，就要指定该用户名称。

7 键入一个端口号或接受默认值。

View 连接服务器使用此端口与 View Composer 服务通信。

8 提供 SSL 证书。

选项	操作
Create default SSL certificate（创建默认 SSL 证书）	选择此单选按钮可为 View Composer 服务创建一个默认的 SSL 证书。 完成安装后，您可以使用由 CA 签发的 SSL 证书替换默认证书。
Use an existing SSL certificate（使用现有 SSL 证书）	如果您安装了 View Composer 服务要使用的 SSL 签名证书，请选择此单选按钮。 从列表中选择一个 SSL 证书。

9 单击**安装**和**完成**以完成 View Composer 服务的安装。

VMware Horizon View Composer 服务即会启动。

View Composer 使用 Windows Server 操作系统提供的加密密码套件。您应遵循贵组织的指导方针来管理 Windows Server 系统上的密码套件。如果贵组织未提供指导方针，VMware 建议您禁用 View Composer Server 上的弱加密密码套件，以增强 Horizon 7 环境的安全。有关管理加密密码套件的信息，请参阅您的 Microsoft 文档。

后续步骤

如果您拥有旧版 vCenter Server，请参阅对从 View Composer 进行的 vCenter 和 ESXi 连接启用 TLSv1.0。

如果手动设置 SQL Server 数据库权限并将其分配给用户，则可撤销该用户的数据库管理员角色。有关更多信息，请参阅（可选）通过手动创建数据库角色设置 SQL Server 数据库权限中过程的最后一步。

对从 View Composer 进行的 vCenter 和 ESXi 连接启用 TLSv1.0

默认情况下，Horizon 7 及更高版本的组件会禁用 TLSv1.0 安全协议。如果您的部署包括仅支持 TLSv1.0 的旧版 vCenter Server，则在安装或升级到 View Composer 7.0 或更高版本后，您可能需要为 View Composer 连接启用 TLSv1.0。

vCenter Server 5.0、5.1 和 5.5 的一些早期维护版本仅支持 TLSv1.0，而在 Horizon 7 及更高版本中默认将不再启用该版本的安全协议。如果无法将 vCenter Server 升级到支持 TLSv1.1 或 TLSv1.2 的版本，则您可以为 View Composer 连接启用 TLSv1.0。

如果您的 ESXi 主机运行的不是 ESXi 6.0 U1b 或更高版本，并且无法进行升级，则您可能还需要启用从 View Composer 到 ESXi 主机的 TLSv1.0 连接。

前提条件

- 确认您已安装 View Composer 7.0 或更高版本。
- 确认您能够以管理员身份登录到 View Composer 计算机，以便使用 Windows 注册表编辑器。

步骤

1 在托管 View Composer 的计算机上，打开 Windows 注册表编辑器 (`regedit.exe`)。

2 导航至 `HKLM\System\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.0\Client`。

如果尚不存在此注册表项，请进行创建。

3 如果存在此注册表项，请删除值 **Enabled**。

4 创建或编辑 **DWORD** 值 **DisabledByDefault**，并将其设置为 **0**。

5 重新启动 VMware Horizon View Composer 服务。

现在已启用从 View Composer 到 vCenter 的 TLSv1.0 连接。

6 在 View Composer 计算机上的 Windows 注册表中，导航至 `HKLM\SOFTWARE\VMware, Inc.\VMware View Composer`。

7 创建或编辑字符串值 **EnableTLS1.0**，并将其设置为 **1**。

8 如果 View Composer 主机是 64 位计算机，请导航到 `HKLM\SOFTWARE\WOW6432Node\VMware, Inc\VMware View Composer`。

9 创建或编辑字符串值 **EnableTLS1.0**，并将其设置为 **1**。

10 重新启动 VMware Horizon View Composer 服务。

现在已启用从 View Composer 到 ESXi 主机的 TLSv1.0 连接。

为 View Composer 配置基础架构

您可以利用 vSphere、vCenter Server、Active Directory 和基础架构的其他组件中的功能来优化 View Composer 的性能、可用性和可靠性。

为 View Composer 配置 vSphere 环境

要支持 View Composer，您需要在安装和配置 vCenter Server、ESXi 和其他 vSphere 组件时遵循某些最佳实践。

这些最佳实践可让 View Composer 在 vSphere 环境中高效运行。

- 创建链接克隆虚拟机的路径和文件夹信息后，不要在 vCenter Server 中更改这些信息，而是应使用 Horizon Administrator 更改文件夹信息。

  如果您在 vCenter Server 中更改此信息，Horizon 7 将找不到 vCenter Server 中的虚拟机。

- 确保为 ESXi 主机上的虚拟交换机设置所配置的端口数足以支持在 ESXi 主机上运行的链接克隆虚拟机配置的所有虚拟网卡。

- 在资源池中部署链接克隆桌面时，请确保您的 vSphere 环境拥有足够的 CPU 和内存来托管所需数量的桌面。使用 vSphere Client 来监视资源池的 CPU 和内存的使用情况。

- 在 vSphere 5.1 及更高版本中，如果副本磁盘存储在 VMFS5 或更高版本的数据存储或 NFS 数据存储中，则用于 View Composer 链接克隆的群集可以包含八台以上的 ESXi 主机。如果您将副本磁盘存储在 VMFS5 之前的版本中，群集最多可包含 8 台主机。

- 使用 vSphere DRS。DRS 可有效地在您的主机之间分配链接克隆虚拟机。

  注 链接克隆桌面不支持 Storage vMotion。

View Composer 的其他最佳实践

要确保 View Composer 高效运行，请检查您的动态名称服务 (dynamic name service, DNS) 是否正确运行，并交错时间运行防病毒软件扫描。

通过确保 DNS 解析正常运行，您可以克服由 DNS 错误导致的断续问题。View Composer 服务依靠动态名称解析来与其他计算机通信。要测试 DNS 的运行，可按名称对 Active Directory 和 View 连接服务器计算机执行 Ping 操作。

如果交错运行防病毒软件，链接克隆桌面的性能将不会受到影响。如果同时在所有链接克隆中运行防病毒软件，则存储子系统上的每秒 I/O 操作 (IOPS) 将会过多。这样的频繁活动会影响链接克隆桌面的性能。

安装 Horizon 连接服务器

7

要使用连接服务器，您需要在支持的计算机上安装相应的软件、配置所需的组件并（可选）优化组件。

本章讨论了以下主题：

- 安装 Horizon 连接服务器软件
- 安装 Horizon 连接服务器的前提条件
- 使用新配置安装 Horizon 连接服务器
- 安装 Horizon 连接服务器副本实例
- 配置安全服务器的配对密码
- 安装安全服务器
- Unified Access Gateway 设备优于 VPN 的方面
- Horizon 连接服务器的防火墙规则
- 使用备份配置重新安装 Horizon 连接服务器
- Microsoft Windows Installer 命令行选项
- 使用 MSI 命令行选项静默卸载 Horizon 7 组件

安装 Horizon 连接服务器软件

根据 Horizon 7 部署的性能、可用性和安全性需求，您可以安装一个连接服务器实例以及多个连接服务器副本实例和安全服务器。您必须至少安装一个连接服务器实例。

安装连接服务器时，需要选择一种安装类型。

标准安装	使用新的 View LDAP 配置生成一个连接服务器实例。
副本安装	使用从现有实例复制的 View LDAP 配置生成一个连接服务器实例。

安全服务器安装	生成一个可在 Internet 和您的内部网络之间添加一层额外安全保护的连接服务器实例。
注册服务器安装	安装 True SSO（单点登录）功能所需的注册服务器，以便用户在登录到 VMware Identity Manager 后，可以连接到远程桌面或应用程序，而无需提供 Active Directory 凭据。注册服务器会请求获取用于身份验证的短期证书。 **注** 由于此功能还要求设置证书颁发机构和执行特定的配置，因此注册服务器的安装过程在《Horizon 7 管理指南》文档的“在不需要凭据的情况下对用户进行身份验证”一章中提供，而未在此安装文档中提供。

安装 Horizon 连接服务器的前提条件

安装连接服务器前，您必须验证安装环境是否符合特定的安装前提条件。

- 您必须具有 Horizon 7 的有效许可证密钥。
- 您必须将连接服务器主机加入到 Active Directory 域。连接服务器支持以下 Active Directory 域服务 (AD DS) 域功能级别：
  - Windows Server 2008
  - Windows Server 2008 R2
  - Windows Server 2012
  - Windows Server 2012 R2
  - Windows Server 2016

  连接服务器主机不能是域控制器。

  注 连接服务器不会也不要求对 Active Directory 进行任何架构或配置更新。
- 不要在安装了 Windows 终端服务器角色的系统上安装连接服务器。您必须从要安装连接服务器的任何系统中移除 Windows 终端服务器角色。
- 不要在执行任何其他功能或角色的系统上安装连接服务器。例如，不要使用同一系统来托管 vCenter Server。
- 要安装连接服务器的系统必须具有一个固定的 IP 地址。在 IPv4 环境中，配置静态 IP 地址。在 IPv6 环境中，计算机会自动获取不会发生更改的 IP 地址。
- 要运行 Horizon 连接服务器安装程序，您必须使用在系统上具有管理员特权的域用户帐户。
- 安装连接服务器时，您会授权一个管理员帐户。您可以指定本地 Administrators 用户组、域用户或用户组帐户。Horizon 7 仅为此帐户分配所有管理权限，包括安装连接服务器副本实例的权限。如果要指定域用户或用户组，则必须先在 Active Directory 中创建帐户，然后再运行安装程序。

使用新配置安装 Horizon 连接服务器

要作为单个服务器或连接服务器副本实例组中的首个实例来安装连接服务器，您可以使用标准安装选项。

选择标准选项时，安装程序会创建一个新的本地 View LDAP 配置。安装程序会加载架构定义、目录信息树 (DIT) 定义和 ACL，并初始化数据。

安装后，您可以使用 Horizon Administrator 管理大多数 View LDAP 配置数据。连接服务器会自动维护部分 View LDAP 条目。

连接服务器软件无法与任何其他 Horizon 7 软件组件（包括副本服务器、安全服务器、View Composer、Horizon Agent 或 Horizon Client）共存于同一虚拟机或物理机上。

使用新配置安装连接服务器时，您可以参加客户体验提升计划。VMware 会收集与您的部署相关的匿名数据，以期更好地响应用户需求。不会收集识别您的组织身份的数据。如果不想参加这一计划，您可以在安装过程中取消选中此选项。如果在安装后改变主意，可以通过编辑 Horizon Administrator 中的“产品许可和使用情况”页面加入或退出计划。要查看从中收集数据的字段列表，包括匿名收集数据的字段，请参阅《Horizon 7 管理指南》文档中的“客户体验提升计划所收集的信息”。

默认情况下，HTML Access 组件会在您安装连接服务器时安装在连接服务器主机上。此组件可配置 Horizon 7 用户门户页面除了显示 Horizon Client 图标之外还显示 HTML Access 图标。用户在连接桌面时可以通过此附加图标选择 HTML Access。

有关为 HTML Access 设置连接服务器的概述，请参阅位于 Horizon Client 文档页面上的《VMware Horizon HTML Access 安装和设置指南》文档。

前提条件

- 确认您能够在安装连接服务器的 Windows Server 计算机上以具有管理员特权的域用户身份登录。
- 确认您的安装符合 Horizon 连接服务器的要求中所述的要求。
- 准备环境以进行安装。请参阅安装 Horizon 连接服务器的前提条件。
- 如果您打算授权域用户或用户组作为管理员帐户，请确认您是在 Active Directory 中创建的域帐户。
- 准备一个数据恢复密码。备份连接服务器时，View LDAP 配置将导出为加密的 LDIF 数据。要恢复加密的备份 Horizon 7 配置，必须提供数据恢复密码。密码包含的字符必须介于 1 到 128 个之间。请遵循组织的最佳实践来生成安全密码。

  重要 您需要数据恢复密码来保持 Horizon 7 的正常运行，并避免业务连续性和灾难恢复 (BCDR) 情形下出现停机。在安装连接服务器时，可以提供一个密码提示。

- 熟悉那些必须在 Windows 防火墙上为连接服务器实例打开的网络端口。请参阅 Horizon 连接服务器的防火墙规则。
- 如果您计划将一台安全服务器与此连接服务器实例配对，请确认活动配置文件中的高级安全 Windows 防火墙已设置为**打开**。建议针对所有配置文件将此设置配置为**打开**。默认情况下，IPsec 规则将管理安全服务器与连接服务器之间的连接，并要求启用“高级安全 Windows 防火墙”。
- 如果您的网络拓扑在安全服务器与连接服务器实例之间包含后端防火墙，则必须将防火墙配置为支持 IPsec。请参阅配置后端防火墙以支持 IPsec。

步骤

1 从 VMware 下载站点下载连接服务器安装程序文件，网址为 https://my.vmware.com/web/vmware/downloads。

在“桌面和最终用户计算”下，选择 VMware Horizon 7 下载，其中包含连接服务器。

安装程序文件名为 `VMware-viewconnectionserver-x86_64-y.y.y-xxxxxx.exe`，其中 *xxxxxx* 为内部版本号，*y.y.y* 为版本号。

2 要启动连接服务器安装程序，请双击安装程序文件。

3 接受 VMware 许可条款。

4 接受或更改目标文件夹。

5 选择 **View 标准服务器**安装选项。

6 选择 Internet 协议 (IP) 版本（**IPv4** 或 **IPv6**）。

必须使用同一 IP 版本安装所有 Horizon 7 组件。

7 选择启用还是禁用 FIPS 模式。

仅当在 Windows 中启用 FIPS 模式时，此选项才可用。

8 如果要允许用户使用 Web 浏览器连接其桌面，应确保选择了**安装 HTML Access**。

如果选择 **IPv4**，将默认选中此设置。由于 IPv6 环境不支持 HTML Access，如果选择 **IPv6**，将不显示此设置。

9 键入数据恢复密码和密码提示（可选）。

10 选择 Windows 防火墙服务的配置方法。

选项	操作
自动配置 Windows 防火墙	让安装程序将 Windows 防火墙配置为允许所需的网络连接。
Do not configure Windows Firewall（不配置 Windows 防火墙）	手动配置 Windows 防火墙规则。 仅当贵组织使用自己预定义的规则来配置 Windows 防火墙时才需要选择此选项。

11 授权 Horizon 管理员帐户。

只有该帐户的成员才可以登录 Horizon Administrator，行使所有管理权限，以及安装连接服务器副本实例和其他 Horizon 7 Server。

选项	说明
授权本地 Administrators 组	允许本地 Administrators 组中的用户管理 Horizon 7。
授权特定的域用户或域组	允许指定的域用户或组管理 Horizon 7。

12 如果您指定了一个域 Horizon 管理员帐户，并且正在以本地管理员或其他没有域帐户访问权限的用户身份运行安装程序，请提供使用授权用户名和密码登录域所需的凭据。

使用 *`domain name\user name`* 或用户主体名称 (UPN) 格式。UPN 格式可以是 *`user@domain.com`*。

13 选择是否参加客户体验提升计划。

如果参加，您可以选择贵组织的类型、规模和所在地。

14 完成安装向导以完成连接服务器的安装。

15 检查 Windows Server 计算机是否有新的修补程序，并根据需要运行 Windows Update。

即使您在安装连接服务器之前完全修补了 Windows Server 计算机，安装过程仍可能会首次启用一些操作系统功能。这样就可能需要额外的修补。

以下 Horizon 7 服务安装在 Windows Server 计算机中：

- VMware Horizon 连接服务器
- VMware Horizon View Framework 组件
- VMware Horizon View Message Bus 组件
- VMware Horizon View 脚本主机
- VMware Horizon View Security Gateway 组件
- VMware Horizon View PCoIP 安全网关
- VMware Horizon View Blast 安全网关
- VMware Horizon View Web 组件
- VMware VDMDS（提供 View LDAP 目录服务）

有关这些服务的信息，请参阅《Horizon 7 管理指南》文档。

如果在安装期间选择了**安装 HTML Access** 设置，则将在 Windows Server 计算机上安装 HTML Access 组件。此组件会在 Horizon 7 用户门户页面中配置 HTML Access 图标，并在 Windows 防火墙中启用 **VMware Horizon View 连接服务器 (内置 Blast)** 规则。此防火墙规则允许客户端设备上的 Web 浏览器在 TCP 端口 8443 上连接到连接服务器。

后续步骤

为连接服务器配置 SSL 服务器证书。请参阅第 8 章，为 Horizon 7 Server 配置 TLS 证书。

如果您拥有旧版 vCenter Server，请参阅对从连接服务器进行的 vCenter 连接启用 TLSv1.0。

在连接服务器上执行初始配置。请参阅第 10 章，首次配置 Horizon 7。

如果您计划在部署中包含连接服务器副本实例和安全服务器，您必须通过运行连接服务器安装程序文件来安装每个服务器实例。

如果您正在重新安装连接服务器且拥有一个配置为监视性能数据的数据收集器组，请停止该数据收集器组后再将其重新启动。

静默安装 Horizon 连接服务器

您可以使用 Microsoft Windows Installer (MSI) 的静默安装功能，在多个 Windows 计算机上执行连接服务器的标准安装。在静默安装中，您需要使用命令行，无需响应向导的提示。

通过静默安装，您可以在大型企业中高效部署 Horizon 7 组件。

前提条件

- 确认您能够在安装连接服务器的 Windows Server 计算机上以具有管理员特权的域用户身份登录。
- 确认您的安装符合 Horizon 连接服务器的要求中所述的要求。
- 准备环境以进行安装。请参阅安装 Horizon 连接服务器的前提条件。
- 如果您打算授权域用户或用户组作为 Horizon 管理员帐户，请确认您是在 Active Directory 中创建的域帐户。
- 如果您使用 MIT Kerberos 身份验证登录到要安装连接服务器的 Windows Server 2008 R2 计算机，请安装知识库文章 978116 中介绍的 Microsoft 修补程序，网址为 http://support.microsoft.com/kb/978116。
- 熟悉那些必须在 Windows 防火墙上为连接服务器实例打开的网络端口。请参阅 Horizon 连接服务器的防火墙规则。
- 如果您计划将一台安全服务器与此连接服务器实例配对，请确认活动配置文件中的高级安全 Windows 防火墙已设置为**打开**。建议针对所有配置文件将此设置配置为**打开**。默认情况下，IPsec 规则将管理安全服务器与连接服务器之间的连接，并要求启用“高级安全 Windows 防火墙”。
- 如果您的网络拓扑在安全服务器与连接服务器实例之间包含后端防火墙，则必须将防火墙配置为支持 IPsec。请参阅配置后端防火墙以支持 IPsec。
- 确认安装连接服务器的 Windows 计算机具有 MSI 运行时引擎 2.0 版或更高版本。有关详细信息，请参见 Microsoft 网站。
- 熟悉 MSI 安装程序命令行选项。请参阅 Microsoft Windows Installer 命令行选项。
- 熟悉连接服务器标准安装可用的静默安装属性。请参阅 Horizon 连接服务器标准安装的静默安装属性。

步骤

1 从 VMware 下载站点下载连接服务器安装程序文件，网址为 https://my.vmware.com/web/vmware/downloads。

在“桌面和最终用户计算”下，选择 VMware Horizon 7 下载，其中包含连接服务器。

安装程序文件名为 `VMware-viewconnectionserver-x86_64-y.y.y-xxxxxx.exe`，其中 *xxxxxx* 为内部版本号，*y.y.y* 为版本号。

2 在 Windows Server 计算机上开启命令提示符。

3 在一行中键入安装命令。

例如：
```
VMware-viewconnectionserver-y.y.y-xxxxxx.exe /s /v"/qn
VDM_SERVER_INSTANCE_TYPE=1 VDM_INITIAL_ADMIN_SID=S-1-5-32-544
VDM_SERVER_RECOVERY_PWD=mini VDM_SERVER_RECOVERY_PWD_REMINDER=""First car"""
```

重要 执行静默安装时，完整的命令行（包括数据恢复密码）会记录在安装程序的 `vminst.log` 文件中。安装完成后，请删除此日志文件或使用 Horizon Administrator 更改数据恢复密码。

4 检查 Windows Server 计算机是否有新的修补程序，并根据需要运行 Windows Update。

即使您在安装连接服务器之前完全修补了 Windows Server 计算机，安装过程仍可能会首次启用一些操作系统功能。这样就可能需要额外的修补。

以下 Horizon 7 服务安装在 Windows Server 计算机中：

- VMware Horizon 连接服务器
- VMware Horizon View Framework 组件
- VMware Horizon View Message Bus 组件
- VMware Horizon View 脚本主机
- VMware Horizon View Security Gateway 组件
- VMware Horizon View PCoIP 安全网关
- VMware Horizon View Blast 安全网关
- VMware Horizon View Web 组件
- VMware VDMDS（提供 View LDAP 目录服务）

如果在安装期间选择了**安装 HTML Access** 设置，则将在 Windows Server 计算机上安装 HTML Access 组件。此组件会在 Horizon 7 用户门户页面中配置 HTML Access 图标，并在 Windows 防火墙中启用 **VMware Horizon View 连接服务器 (内置 Blast)** 规则。此防火墙规则允许客户端设备上的 Web 浏览器在 TCP 端口 8443 上连接到连接服务器。

有关这些服务的信息，请参阅《Horizon 7 管理指南》文档。

后续步骤

为连接服务器配置 SSL 服务器证书。请参阅第 8 章，为 Horizon 7 Server 配置 TLS 证书。

如果您拥有旧版 vCenter Server，请参阅对从连接服务器进行的 vCenter 连接启用 TLSv1.0。

如果您是首次配置 Horizon 7，请在连接服务器上执行初始配置。请参阅第 10 章，首次配置 Horizon 7。

Horizon 连接服务器标准安装的静默安装属性

从命令行执行静默安装时，可以包含特定的连接服务器属性。您必须使用 *PROPERTY=value* 的格式，以便 Microsoft Windows Installer (MSI) 理解各属性和值。

表 7-1. 在标准安装中静默安装连接服务器的 MSI 属性

MSI 属性	说明	默认值
INSTALLDIR	连接服务器软件的安装路径和文件夹。 例如：`INSTALLDIR=""D:\abc\my folder""` 路径由两对双引号括起，允许 MSI 安装程序将其中的空格视为路径的有效部分。	`%ProgramFiles%\VMware\VMware View\Server`
VDM_SERVER_INSTANCE_TYPE	Horizon Server 的安装类型包括： ■ **1**. 标准安装 ■ **2**.副本安装 ■ **3**.安全服务器安装 ■ **5**. 注册服务器安装 例如，要执行标准安装，请定义 `VDM_SERVER_INSTANCE_TYPE=1`	1
FWCHOICE	确定是否为连接服务器实例配置防火墙的 MSI 属性。 值为 1 时表示配置防火墙。值为 2 时表示不配置防火墙。 例如：`FWCHOICE=1`	1
VDM_INITIAL_ADMIN_SID	已被授权完整 Horizon 管理权限的初始 Horizon Administrator 用户或用户组的 SID。 默认值为连接服务器计算机上的本地 Administrators 用户组的 SID。您可以指定域用户或用户组帐户的 SID。	`S-1-5-32-544`
VDM_SERVER_RECOVERY_PWD	数据恢复密码。如果未在 Horizon LDAP 中设置数据恢复密码，则必须配置此属性。 密码包含的字符必须介于 1 到 128 个之间。请遵循组织的最佳实践来生成安全密码。	无
VDM_SERVER_RECOVERY_PWD_REMINDER	数据恢复密码提示。此属性是可选的。	无
VDM_IP_PROTOCOL_用途	指定 Horizon 组件用于通信的 IP 版本。可能的值为 **IPv4** 和 **IPv6**。	**IPv4**
VDM_FIPS_ENABLED	指定启用还是禁用 FIPS 模式。值为 1 将启用 FIPS 模式。值为 0 将禁用 FIPS 模式。如果此属性设置为 1 并且 Windows 未处于 FIPS 模式中，则安装程序将中止。	0
HTMLACCESS	控制 HTML Access 加载项安装。将该属性设置为 1 以配置 HTML Access，或者在不需要使用 HTML Access 时忽略该属性。	1

对从连接服务器进行的 vCenter 连接启用 TLSv1.0

默认情况下，Horizon 7 及更高版本的组件会禁用 TLSv1.0 安全协议。如果您的部署包括仅支持 TLSv1.0 的旧版 vCenter Server，则在安装或升级到连接服务器 7.0 或更高版本后，您可能需要为连接服务器连接启用 TLSv1.0。

vCenter Server 5.1 和 5.5 的一些早期维护版本仅支持 TLSv1.0，而在 Horizon 7 及更高版本中默认将不再启用该版本的安全协议。如果无法将 vCenter Server 升级到支持 TLSv1.1 或 TLSv1.2 的版本，则您可以为连接服务器连接启用 TLSv1.0。

前提条件

- 如果您要升级到 Horizon 7，请在升级之前执行此过程，以便最大限度地减少需要重新启动服务的次数。在升级期间，将会重新启动连接服务器服务，而且要应用此过程中所述的配置更改，也需要重新启动该服务。如果在执行此过程之前进行升级，则您将需要再次重新启动该服务。
- 请参阅 Microsoft TechNet 网站，了解如何在您的 Windows 操作系统版本上使用“ADSI 编辑”实用程序。

步骤

1 在您的连接服务器主机上启动“ADSI 编辑”实用程序。

2 在控制台树中，选择**连接到**。

3 在**选择或键入可分辨名称或命名上下文**文本框中，键入可分辨名称 **DC=vdi, DC=vmware, DC=int**。

4 在“计算机”窗格中，选择或键入 **localhost:389** 或者连接服务器主机的完全限定域名 (Fully Qualified Domain Name, FQDN) 后跟端口 389。

   例如：**localhost:389** 或 **mycomputer.example.com:389**。

5 展开“ADSI 编辑”树，展开 **OU=Properties**，选择 **OU=Global**，然后在右侧窗格中双击 **CN=Common**。

6 在“属性”对话框中，编辑 **pae-ClientSSLSecureProtocols** 属性以添加下列值：

   \LIST:TLSv1.2,TLSv1.1,TLSv1

   请确保在行首包括反斜杠。

7 单击**确定**。

8 如果这是全新安装，则要应用配置更改，需重新启动每个连接服务器实例上的连接服务器服务。

   如果您计划执行升级，则无需重新启动该服务，因为升级过程会自动重新启动该服务。

安装 Horizon 连接服务器副本实例

要提供高可用性和负载平衡功能，您可以安装一个或多个复制现有连接服务器实例的其他连接服务器实例。在完成副本安装后，现有及新安装的连接服务器实例将完全相同。

安装副本实例时，Horizon 7 会从现有连接服务器实例复制 View LDAP 配置数据。

安装后，副本组中所有连接服务器实例上的 View LDAP 配置数据均保持相同。更改一个实例时，更新的信息将复制到其他实例。

如果一个副本实例出现故障，组中的其他实例会继续运行。当出现故障的实例恢复活动时，其配置数据将自动更新，以对故障期间发生的更改进行同步。

注 复制功能由 View LDAP 提供，LDAP 使用的复制技术与 Active Directory 所用技术相同。

副本服务器软件无法与任何其他 Horizon 7 软件组件（包括安全服务器、连接服务器、View Composer、Horizon Agent 或 Horizon Client）共存于同一虚拟机或物理机上。

默认情况下，HTML Access 组件会在您安装连接服务器时安装在连接服务器主机上。此组件可配置 Horizon 7 用户门户页面除了显示 Horizon Client 图标之外还显示 HTML Access 图标。用户在连接桌面时可以通过此附加图标选择 HTML Access。

有关为 HTML Access 设置连接服务器的概述，请参阅位于 Horizon Client 文档页面上的《VMware Horizon HTML Access 安装和设置指南》文档。

前提条件

- 确认网络上至少已安装并配置了一个连接服务器实例。
- 要安装副本实例，您必须以具有管理员角色的用户身份登录。具有管理员角色的帐户或组是在安装连接服务器的第一个实例时指定的。该角色可以分配给本地 Administrators 组、域用户或组。请参阅使用新配置安装 Horizon 连接服务器。
- 如果现有的连接服务器实例所在的域与副本实例的域不同，域用户还必须在安装了现有实例的 Windows Server 计算机上具有管理员特权。
- 如果您使用 MIT Kerberos 身份验证登录到要安装连接服务器的 Windows Server 2008 R2 计算机，请安装知识库文章 978116 中介绍的 Microsoft 修补程序，网址为 http://support.microsoft.com/kb/978116。
- 确认您的安装符合 Horizon 连接服务器的要求中所述的要求。
- 确认安装连接服务器副本实例的计算机已连接到高性能 LAN。请参阅 Horizon 连接服务器副本实例的网络要求。
- 准备环境以进行安装。请参阅安装 Horizon 连接服务器的前提条件。
- 如果安装的连接服务器副本实例为 Horizon 7 5.1 或更高版本，而要复制的现有连接服务器实例为 Horizon 7 5.0.*x* 或更低版本，请准备一个数据恢复密码。请参阅使用新配置安装 Horizon 连接服务器。
- 熟悉那些必须在 Windows 防火墙上为连接服务器实例打开的网络端口。请参阅 Horizon 连接服务器的防火墙规则。
- 如果您计划将一台安全服务器与此连接服务器实例配对，请确认活动配置文件中的高级安全 Windows 防火墙已设置为**打开**。建议针对所有配置文件将此设置配置为**打开**。默认情况下，IPsec 规则将管理安全服务器与连接服务器之间的连接，并要求启用“高级安全 Windows 防火墙”。
- 如果您的网络拓扑在安全服务器与连接服务器实例之间包含后端防火墙，则必须将防火墙配置为支持 IPsec。请参阅配置后端防火墙以支持 IPsec。

步骤

1 从 VMware 下载站点下载连接服务器安装程序文件，网址为 https://my.vmware.com/web/vmware/downloads。

在“桌面和最终用户计算”下，选择 VMware Horizon 7 下载，其中包含连接服务器。

安装程序文件名为 `VMware-viewconnectionserver-x86_64-y.y.y-xxxxxx.exe`，其中 *xxxxxx* 为内部版本号，*y.y.y* 为版本号。

2 要启动连接服务器安装程序，请双击安装程序文件。

3 接受 VMware 许可条款。

4 接受或更改目标文件夹。

5 选择 **View 副本服务器**安装选项。

6 选择 Internet 协议 (IP) 版本（**IPv4** 或 **IPv6**）。

必须使用同一 IP 版本安装所有 Horizon 7 组件。

7 选择启用还是禁用 FIPS 模式。

仅当在 Windows 中启用 FIPS 模式时，此选项才可用。

8 如果要允许用户使用 HTML Access 连接其桌面，应确保选择了**安装 HTML Access**。

如果选择 **IPv4**，将默认选中此设置。由于 IPv6 环境不支持 HTML Access，如果选择 **IPv6**，将不显示此设置。

9 输入要复制的现有连接服务器实例的主机名或 IP 地址。

10 键入数据恢复密码和密码提示（可选）。

仅当您要复制的现有连接服务器实例为 Horizon 7 5.0.*x* 或更低版本时，系统才会提示您输入数据恢复密码。

11 选择 Windows 防火墙服务的配置方法。

选项	操作
自动配置 Windows 防火墙	让安装程序将 Windows 防火墙配置为允许所需的网络连接。
Do not configure Windows Firewall（不配置 Windows 防火墙）	手动配置 Windows 防火墙规则。 仅当贵组织使用自己预定义的规则来配置 Windows 防火墙时才需要选择此选项。

12 完成安装向导以完成安装副本实例。

13 检查 Windows Server 计算机是否有新的修补程序，并根据需要运行 Windows Update。

即使您在安装连接服务器之前完全修补了 Windows Server 计算机，安装过程仍可能会首次启用一些操作系统功能。这样就可能需要额外的修补。

以下 Horizon 7 服务安装在 Windows Server 计算机中：

- VMware Horizon 连接服务器
- VMware Horizon View Framework 组件
- VMware Horizon View Message Bus 组件
- VMware Horizon View 脚本主机
- VMware Horizon View Security Gateway 组件
- VMware Horizon View PCoIP 安全网关
- VMware Horizon View Blast 安全网关
- VMware Horizon View Web 组件
- VMware VDMDS（提供 View LDAP 目录服务）

有关这些服务的信息，请参阅《Horizon 7 管理指南》文档。

如果在安装期间选择了**安装 HTML Access** 设置，则将在 Windows Server 计算机上安装 HTML Access 组件。此组件会在 Horizon 7 用户门户页面中配置 HTML Access 图标，并在 Windows 防火墙中启用 **VMware Horizon View 连接服务器 (内置 Blast)** 规则。此防火墙规则允许客户端设备上的 Web 浏览器在 TCP 端口 8443 上连接到连接服务器。

后续步骤

为连接服务器实例配置 SSL 服务器证书。请参阅第 8 章，为 Horizon 7 Server 配置 TLS 证书。

您无需在连接服务器副本实例上执行初始 Horizon 7 配置。副本实例会从现有连接服务器实例继承配置。

但是，您可能需要为此连接服务器实例配置客户端连接设置，同时可以调整 Windows Server 设置以支持大规模部署。请参阅配置 Horizon Client 连接和调整 Windows Server 设置以支持您的部署。

如果您正在重新安装连接服务器且拥有一个配置为监视性能数据的数据收集器组，请停止该数据收集器组后再将其重新启动。

静默安装 Horizon 连接服务器副本实例

您可以使用 Microsoft Windows Installer (MSI) 的静默安装功能，在多个 Windows 计算机上安装连接服务器副本实例。在静默安装中，您需要使用命令行，无需响应向导的提示。

通过静默安装，您可以在大型企业中高效部署 Horizon 7 组件。

前提条件

- 确认网络上至少已安装并配置了一个连接服务器实例。
- 要安装副本实例，您必须以具有管理员帐户访问凭据的用户身份登录。管理员帐户是在安装连接服务器的第一个实例时指定的。该帐户可以是本地 Administrators 用户组、域用户或用户组帐户。请参阅使用新配置安装 Horizon 连接服务器。
- 如果现有的连接服务器实例所在的域与副本实例的域不同，域用户还必须在安装了现有实例的 Windows Server 计算机上具有管理员特权。
- 如果您使用 MIT Kerberos 身份验证登录到要安装连接服务器的 Windows Server 2008 R2 计算机，请安装知识库文章 978116 中介绍的 Microsoft 修补程序，网址为 http://support.microsoft.com/kb/978116。
- 确认您的安装符合 Horizon 连接服务器的要求中所述的要求。
- 确认安装连接服务器副本实例的计算机已连接到高性能 LAN。请参阅 Horizon 连接服务器副本实例的网络要求。
- 准备环境以进行安装。请参阅安装 Horizon 连接服务器的前提条件。
- 熟悉那些必须在 Windows 防火墙上为连接服务器实例打开的网络端口。请参阅 Horizon 连接服务器的防火墙规则。
- 如果您计划将一台安全服务器与此连接服务器实例配对，请确认活动配置文件中的高级安全 Windows 防火墙已设置为**打开**。建议针对所有配置文件将此设置配置为**打开**。默认情况下，IPsec 规则将管理安全服务器与连接服务器之间的连接，并要求启用“高级安全 Windows 防火墙”。

- 如果您的网络拓扑在安全服务器与连接服务器实例之间包含后端防火墙，则必须将防火墙配置为支持 IPsec。请参阅配置后端防火墙以支持 IPsec。
- 熟悉 MSI 安装程序命令行选项。请参阅 Microsoft Windows Installer 命令行选项。
- 熟悉连接服务器副本安装可用的静默安装属性。请参阅 Horizon 连接服务器副本实例的静默安装属性。

步骤

1 从 VMware 下载站点下载连接服务器安装程序文件，网址为 https://my.vmware.com/web/vmware/downloads。

在“桌面和最终用户计算”下，选择 VMware Horizon 7 下载，其中包含连接服务器。

安装程序文件名为 `VMware-viewconnectionserver-x86_64-y.y.y-xxxxxx.exe`，其中 *xxxxxx* 为内部版本号，*y.y.y* 为版本号。

2 在 Windows Server 计算机上开启命令提示符。

3 在一行中键入安装命令。

例如：
```
VMware-viewconnectionserver-y.y.y-xxxxxx.exe /s /v"/qn
VDM_SERVER_INSTANCE_TYPE=2 ADAM_PRIMARY_NAME=cs1.companydomain.com
VDM_INITIAL_ADMIN_SID=S-1-5-32-544"
```

如果安装的连接服务器副本实例为 View 5.1 或更高版本，而要复制的现有连接服务器实例为 View 5.0.*x* 或更低版本，则必须指定数据恢复密码，您可以添加一个密码提示。例如：
```
VMware-viewconnectionserver-y.y.y-xxxxxx.exe /s /v"/qn VDM_SERVER_INSTANCE_TYPE=2
ADAM_PRIMARY_NAME=cs1.companydomain.com VDM_INITIAL_ADMIN_SID=S-1-5-32-544
VDM_SERVER_RECOVERY_PWD=mini VDM_SERVER_RECOVERY_PWD_REMINDER=""First car"""
```

重要 执行静默安装时，完整的命令行（包括数据恢复密码）会记录在安装程序的 `vminst.log` 文件中。安装完成后，请删除此日志文件或使用 Horizon Administrator 更改数据恢复密码。

4 检查 Windows Server 计算机是否有新的修补程序，并根据需要运行 Windows Update。

即使您在安装连接服务器之前完全修补了 Windows Server 计算机，安装过程仍可能会首次启用一些操作系统功能。这样就可能需要额外的修补。

以下 Horizon 7 服务安装在 Windows Server 计算机中：

- VMware Horizon 连接服务器
- VMware Horizon View Framework 组件
- VMware Horizon View Message Bus 组件
- VMware Horizon View 脚本主机
- VMware Horizon View Security Gateway 组件
- VMware Horizon View PCoIP 安全网关
- VMware Horizon View Blast 安全网关

- VMware Horizon View Web 组件
- VMware VDMDS（提供 View LDAP 目录服务）

有关这些服务的信息，请参阅《Horizon 7 管理指南》文档。

如果在安装期间选择了**安装 HTML Access** 设置，则将在 Windows Server 计算机上安装 HTML Access 组件。此组件会在 Horizon 7 用户门户页面中配置 HTML Access 图标，并在 Windows 防火墙中启用 **VMware Horizon View 连接服务器 (内置 Blast)** 规则。此防火墙规则允许客户端设备上的 Web 浏览器在 TCP 端口 8443 上连接到连接服务器。

后续步骤

为连接服务器实例配置 SSL 服务器证书。请参阅第 8 章，为 Horizon 7 Server 配置 TLS 证书。

您无需在连接服务器副本实例上执行初始 Horizon 7 配置。副本实例会从现有连接服务器实例继承配置。

但是，您可能需要为此连接服务器实例配置客户端连接设置，同时可以调整 Windows Server 设置以支持大规模部署。请参阅配置 Horizon Client 连接和调整 Windows Server 设置以支持您的部署。

Horizon 连接服务器副本实例的静默安装属性

从命令行执行 Horizon 连接服务器副本实例静默安装时可以包含特定属性。您必须使用 *PROPERTY=value* 的格式，以便 Microsoft Windows Installer (MSI) 理解各属性和值。

表 7-2. 静默安装 Horizon 连接服务器副本实例的 MSI 属性

MSI 属性	说明	默认值
INSTALLDIR	连接服务器软件的安装路径和文件夹。 例如：`INSTALLDIR=""D:\abc\my folder""` 路径由两对双引号括起，允许 MSI 安装程序将其中的空格视为路径的有效部分。 此 MSI 属性是可选的。	`%ProgramFiles%\VMware\VMware View\Server`
VDM_SERVER_INSTANCE_TYPE	连接服务器的安装类型： ■ **1**. 标准安装 ■ **2**.副本安装 ■ **3**.安全服务器安装 要安装副本实例，请定义 `VDM_SERVER_INSTANCE_TYPE=2` 安装副本时，此 MSI 属性是必要属性。	1
ADAM_PRIMARY_NAME	要复制的现有连接服务器实例的主机名或 IP 地址。 例如：`ADAM_PRIMARY_NAME=cs1.companydomain.com` 此 MSI 属性是必要属性。	无
FWCHOICE	确定是否为连接服务器实例配置防火墙的 MSI 属性。 值为 1 时表示配置防火墙。值为 2 时表示不配置防火墙。 例如：`FWCHOICE=1` 此 MSI 属性是可选的。	1

表 7-2. 静默安装 Horizon 连接服务器副本实例的 MSI 属性（续）

MSI 属性	说明	默认值
VDM_SERVER_RECOVERY_PWD	数据恢复密码。如果未在 View LDAP 中设置数据恢复密码，则必须配置此属性。 注 如果要复制的标准连接服务器实例为 View 5.0 或更低版本，则 View LDAP 中未设置数据恢复密码。如果要复制的连接服务器实例为 View 5.1 或更高版本，则无需提供此属性。 密码包含的字符必须介于 1 到 128 个之间。请遵循组织的最佳实践来生成安全密码。	无
VDM_SERVER_RECOVERY_PWD_REMINDER	数据恢复密码提示。此属性是可选的。	无
VDM_IP_PROTOCOL_用途	指定 Horizon 7 组件用于通信的 IP 版本。可能的值为 **IPv4** 和 **IPv6**	**IPv4**
VDM_FIPS_ENABLED	指定启用还是禁用 FIPS 模式。值为 1 将启用 FIPS 模式。值为 0 将禁用 FIPS 模式。如果此属性设置为 1 并且 Windows 未处于 FIPS 模式中，则安装程序将中止。	0

配置安全服务器的配对密码

安装安全服务器之前，您必须配置安全服务器配对密码。在使用连接服务器安装程序安装安全服务器时，程序会在安装过程中提示您输入此密码。

安全服务器配对密码是一次性密码，允许安全服务器与连接服务器实例配对。密码被提供给连接服务器安装程序后，就会变成无效密码。

注 旧版的安全服务器与当前版本的连接服务器不能配对。如果为当前版本的连接服务器配置了配对密码并尝试安装旧版安全服务器，则配对密码将无效。

步骤

1 在 Horizon Administrator 中，选择 **View 配置 > 服务器**。

2 在“连接服务器”选项卡中，选择要与安全服务器配对的连接服务器实例。

3 从 **更多命令**下拉菜单中选择**指定安全服务器配对密码**。

4 在“配对密码”和“确认密码”文本框中分别键入密码并指定密码超时值。

您必须在指定的超时期限内使用密码。

5 单击**确定**配置密码。

后续步骤

安装安全服务器。请参阅安装安全服务器。

重要 如果您在安全服务器配对密码超时期限内未将其提供给连接服务器安装程序，密码会变为无效，且您必须配置一个新密码。

安装安全服务器

安全服务器是一个连接服务器实例，可在 Internet 和您的内部网络之间添加一层额外的安全保护。您可以安装一个或多个安全服务器，以连接到连接服务器实例。

安全服务器软件无法与任何其他 Horizon 7 软件组件（包括副本服务器、连接服务器、View Composer、Horizon Agent 或 Horizon Client）共存于同一虚拟机或物理机上。

前提条件

- 确定要使用的拓扑结构类型。例如，确定所用的负载平衡解决方案。确定与安全服务器配对的连接服务器实例是否专供外部网络用户使用。有关信息，请参阅《Horizon 7 架构规划指南》文档。

  重要 如果使用负载平衡器，则它必须具有不会发生更改的 IP 地址。在 IPv4 环境中，配置静态 IP 地址。在 IPv6 环境中，计算机会自动获取不会发生更改的 IP 地址。

- 确认您的安装符合 Horizon 连接服务器的要求中所述的要求。
- 准备环境以进行安装。请参阅安装 Horizon 连接服务器的前提条件。
- 确认要与安全服务器配对的连接服务器实例已安装并经过配置，且运行的连接服务器版本与安全服务器版本兼容。请参阅《Horizon 7 升级指南》文档中的“Horizon 7 组件兼容性列表”。
- 确认计划安装安全服务器的计算机可以访问要与安全服务器配对的连接服务器实例。

  注 连接服务器升级到 Horizon 7 版本 7.5 后，必须重新安装禁用了 IPsec 的安全服务器。如果安全服务器的 IP 地址发生更改，必须重新安装此服务器。如果安全服务器位于动态 NAT 后面，安全服务器配对功能将无法正常工作。

- 配置安全服务器的配对密码。请参阅配置安全服务器的配对密码。
- 熟悉外部 URL 的格式。请参阅为安全网关和安全加密链路连接配置外部 URL。
- 确认高级安全 Windows 防火墙在活动配置文件中已设置为**打开**。建议针对所有配置文件将此设置配置为**打开**。默认情况下，IPsec 规则会控制安全服务器与 View 连接服务器之间的连接，并要求启用“高级安全 Windows 防火墙”。
- 熟悉那些必须在 Windows 防火墙上为安全服务器打开的网络端口。请参阅 Horizon 连接服务器的防火墙规则。
- 如果您的网络拓扑在安全服务器与连接服务器之间包含后端防火墙，则必须将防火墙配置为支持 IPsec。请参阅配置后端防火墙以支持 IPsec。
- 如果您要升级或重新安装安全服务器，请确认现有的安全服务器 IPsec 规则已移除。请参阅移除安全服务器的 IPsec 规则。
- 如果以 FIPS 模式安装 Horizon 7，则必须在 Horizon Administrator 中取消选择全局设置**使用 IPSec 进行安全服务器连接**，因为在 FIPS 模式中，必须在安装安全服务器后手动配置 IPsec。

步骤

1 从 VMware 下载站点下载连接服务器安装程序文件，网址为 https://my.vmware.com/web/vmware/downloads。

在“桌面和最终用户计算”下，选择 VMware Horizon 7 下载，其中包含连接服务器。

安装程序文件名为 `VMware-viewconnectionserver-x86_64-y.y.y-xxxxxx.exe`，其中 *xxxxxx* 为内部版本号，*y.y.y* 为版本号。

2 要启动连接服务器安装程序，请双击安装程序文件。

3 接受 VMware 许可条款。

4 接受或更改目标文件夹。

5 选择 **View 安全服务器**安装选项。

6 选择 Internet 协议 (IP) 版本（**IPv4** 或 **IPv6**）。

必须使用同一 IP 版本安装所有 Horizon 7 组件。

7 选择启用还是禁用 FIPS 模式。

仅当在 Windows 中启用 FIPS 模式时，此选项才可用。

8 在**服务器**文本框中键入要与安全服务器配对的连接服务器实例的完全限定域名或 IP 地址。

安全服务器会将网络流量转发到此连接服务器实例。

9 在**密码**文本框中键入安全服务器配对密码。

如果密码已过期，可以使用 Horizon Administrator 配置一个新密码，然后在安装程序中键入该新密码。

10 在**外部 URL** 文本框中键入使用 RDP 或 PCoIP 显示协议的客户端终端的安全服务器外部 URL。

URL 必须包含协议、客户端可解析的安全服务器名和端口号。在网络外运行的安全加密链路客户端会使用该 URL 连接安全服务器。

例如：`https://view.example.com:443`

11 在 **PCoIP 外部 URL** 文本框中，键入使用 PCoIP 显示协议的客户端终端的安全服务器外部 URL。

在 IPv4 环境中，指定 PCoIP 外部 URL 作为 IP 地址，端口号为 4172。在 IPv6 环境中，可以指定 IP 地址或完全限定域名，端口号为 4172。在两种环境中，都不要包含协议名称。

例如，在 IPv4 环境中：`10.20.30.40:4172`

客户端必须能够使用 URL 访问安全服务器。

12 在 **Blast 外部 URL** 文本框中，键入使用 HTML Access 连接远程桌面的用户的安全服务器外部 URL。

URL 必须包含 HTTPS 协议、客户端可解析的主机名和端口号。

例如：`https://myserver.example.com:8443`

默认情况下，URL 包含安全加密链路外部 URL 的 FQDN 和默认端口号 8443。URL 必须包含客户端系统可用来连接此安全服务器的 FQDN 和端口号。

13 选择 Windows 防火墙服务的配置方法。

选项	操作
自动配置 Windows 防火墙	让安装程序将 Windows 防火墙配置为允许所需的网络连接。
Do not configure Windows Firewall（不配置 Windows 防火墙）	手动配置 Windows 防火墙规则。 仅当贵组织使用自己预定义的规则来配置 Windows 防火墙时才需要选择此选项。

14 完成安装向导以完成安装安全服务器。

安全服务器服务将安装在 Windows Server 计算机中：

- VMware Horizon View 安全服务器
- VMware Horizon View Framework 组件
- VMware Horizon View Security Gateway 组件
- VMware Horizon View PCoIP 安全网关
- VMware Blast 安全网关

有关这些服务的信息，请参阅《Horizon 7 管理指南》文档。

安全服务器会显示在 Horizon Administrator 的“安全服务器”窗格中。

在安全服务器上的 Windows 防火墙中，**VMware Horizon View 连接服务器 (内置 Blast)** 规则已启用。该防火墙规则允许客户端设备上的 Web 浏览器使用 HTML Access 连接 TCP 端口 8443 上的安全服务器。

注 如果安装取消或中止，可能必须先删除安全服务器的 IPsec 规则，然后才能开始再次安装。即便您在重新安装或升级安全服务器之前已经移除了 IPsec 规则，也要执行此步骤。有关移除 IPsec 规则的说明，请参阅移除安全服务器的 IPsec 规则。

后续步骤

为安全服务器配置 SSL 服务器证书。请参阅第 8 章，为 Horizon 7 Server 配置 TLS 证书。

您可能需要为安全服务器配置客户端连接设置，同时可以调整 Windows Server 设置以支持大规模部署。请参阅配置 Horizon Client 连接和调整 Windows Server 设置以支持您的部署。

如果您重新安装安全服务器且拥有一个配置为监视性能数据的数据收集器组，请停止数据收集器组然后重新启动。

静默安装安全服务器

您可以使用 Microsoft Windows Installer (MSI) 的静默安装功能在多个 Windows 计算机上安装安全服务器。在静默安装中，您需要使用命令行，无需响应向导的提示。

通过静默安装，您可以在大型企业中高效部署 Horizon 7 组件。

前提条件

- 确定要使用的拓扑结构类型。例如，确定所用的负载平衡解决方案。确定与安全服务器配对的连接服务器实例是否专供外部网络用户使用。有关信息，请参阅《Horizon 7 架构规划指南》文档。

  重要 如果使用负载平衡器，则它必须具有不会发生更改的 IP 地址。在 IPv4 环境中，配置静态 IP 地址。在 IPv6 环境中，计算机会自动获取不会发生更改的 IP 地址。

- 确认您的安装符合 Horizon 连接服务器的要求中所述的要求。
- 准备环境以进行安装。请参阅安装 Horizon 连接服务器的前提条件。
- 确认要与安全服务器配对的连接服务器实例已安装并经过配置，且运行的连接服务器版本与安全服务器版本兼容。请参阅《Horizon 7 升级指南》文档中的“Horizon 7 组件兼容性列表”。
- 确认计划安装安全服务器的计算机可以访问要与安全服务器配对的连接服务器实例。

  注 连接服务器升级到 Horizon 7 版本 7.5 后，必须重新安装禁用了 IPsec 的安全服务器。如果安全服务器的 IP 地址发生更改，必须重新安装此服务器。如果安全服务器位于动态 NAT 后面，安全服务器配对功能将无法正常工作。

- 配置安全服务器的配对密码。请参阅配置安全服务器的配对密码。
- 熟悉外部 URL 的格式。请参阅为安全网关和安全加密链路连接配置外部 URL。
- 确认高级安全 Windows 防火墙在活动配置文件中已设置为**打开**。建议针对所有配置文件将此设置配置为**打开**。默认情况下，IPsec 规则将管理安全服务器与连接服务器之间的连接，并要求启用“高级安全 Windows 防火墙”。
- 熟悉那些必须在 Windows 防火墙上为安全服务器打开的网络端口。请参阅 Horizon 连接服务器的防火墙规则。
- 如果您的网络拓扑在安全服务器与连接服务器之间包含后端防火墙，则必须将防火墙配置为支持 IPsec。请参阅配置后端防火墙以支持 IPsec。
- 如果您要升级或重新安装安全服务器，请确认现有的安全服务器 IPsec 规则已移除。请参阅移除安全服务器的 IPsec 规则。
- 熟悉 MSI 安装程序命令行选项。请参阅 Microsoft Windows Installer 命令行选项。
- 熟悉安全服务器可用的静默安装属性。请参阅安全服务器的静默安装属性。
- 如果以 FIPS 模式安装 Horizon 7，则必须在 Horizon Administrator 中取消选择全局设置**使用 IPSec 进行安全服务器连接**，因为在 FIPS 模式中，必须在安装安全服务器后手动配置 IPsec。

步骤

1 从 VMware 下载站点下载连接服务器安装程序文件，网址为 https://my.vmware.com/web/vmware/downloads。

  在“桌面和最终用户计算”下，选择 VMware Horizon 7 下载，其中包含连接服务器。

  安装程序文件名为 `VMware-viewconnectionserver-x86_64-y.y.y-xxxxxx.exe`，其中 *xxxxxx* 为内部版本号，*y.y.y* 为版本号。

2 在 Windows Server 计算机上开启命令提示符。

3 在一行中键入安装命令。

例如：`VMware-viewconnectionserver-y.y.y-xxxxxx.exe /s /v"/qn VDM_SERVER_INSTANCE_TYPE=3 VDM_SERVER_NAME=cs1.internaldomain.com VDM_SERVER_SS_EXTURL=https://view.companydomain.com:443 VDM_SERVER_SS_PCOIP_IPADDR=10.20.30.40 VDM_SERVER_SS_PCOIP_TCPPORT=4172 VDM_SERVER_SS_PCOIP_UDPPORT=4172 VDM_SERVER_SS_BSG_EXTURL=https://view.companydomain.com:8443 VDM_SERVER_SS_PWD=secret"`

安全服务器服务将安装在 Windows Server 计算机中：

- VMware Horizon View 安全服务器
- VMware Horizon View Framework 组件
- VMware Horizon View Security Gateway 组件
- VMware Horizon View PCoIP 安全网关
- VMware Blast 安全网关

有关这些服务的信息，请参阅《Horizon 7 管理指南》文档。

安全服务器会显示在 Horizon Administrator 的“安全服务器”窗格中。

在安全服务器上的 Windows 防火墙中，**VMware Horizon View 连接服务器 (内置 Blast)** 规则已启用。该防火墙规则允许客户端设备上的 Web 浏览器使用 HTML Access 连接 TCP 端口 8443 上的安全服务器。

注 如果安装取消或中止，可能必须先删除安全服务器的 IPsec 规则，然后才能开始再次安装。即便您在重新安装或升级安全服务器之前已经移除了 IPsec 规则，也要执行此步骤。有关移除 IPsec 规则的说明，请参阅移除安全服务器的 IPsec 规则。

后续步骤

为安全服务器配置 SSL 服务器证书。请参阅第 8 章，为 Horizon 7 Server 配置 TLS 证书。

您可能需要为安全服务器配置客户端连接设置，同时可以调整 Windows Server 设置以支持大规模部署。请参阅配置 Horizon Client 连接和调整 Windows Server 设置以支持您的部署。

安全服务器的静默安装属性

从命令行执行安全服务器静默安装时可以包含特定属性。您必须使用 *PROPERTY=value* 的格式，以便 Microsoft Windows Installer (MSI) 理解各属性和值。

表 7-3. 静默安装安全服务器的 MSI 属性

MSI 属性	说明	默认值
INSTALLDIR	连接服务器软件的安装路径和文件夹。 例如：`INSTALLDIR=""D:\abc\my folder""` 路径由两对双引号括起，允许 MSI 安装程序将其中的空格视为路径的有效部分。 此 MSI 属性是可选的。	`%ProgramFiles%\VMware\VMware View\Server`
VDM_SERVER_INSTANCE_TYPE	连接服务器的安装类型： ■ **1**. 标准安装 ■ **2**.副本安装 ■ **3**.安全服务器安装 要安装安全服务器，请定义 `VDM_SERVER_INSTANCE_TYPE=3` 安装安全服务器时，此 MSI 属性是必要属性。	1
VDM_SERVER_NAME	要与安全服务器配对的现有连接服务器实例的主机名或 IP 地址。 例如：`VDM_SERVER_NAME=cs1.internaldomain.com` 此 MSI 属性是必要属性。	无
VDM_SERVER_SS_EXTURL	安全服务器的外部 URL。URL 必须包含协议、可外部解析的安全服务器名和端口号 例如：`VDM_SERVER_SS_EXTURL=https://view.companydomain.com:443` 此 MSI 属性是必要属性。	无
VDM_SERVER_SS_PWD	安全服务器配对密码。 例如：`VDM_SERVER_SS_PWD=secret` 此 MSI 属性是必要属性。	无
FWCHOICE	确定是否为连接服务器实例配置防火墙的 MSI 属性。 值为 1 时表示配置防火墙。值为 2 时表示不配置防火墙。 例如：`FWCHOICE=1` 此 MSI 属性是可选的。	1
VDM_SERVER_SS_PCOIP_IPADDR	PCoIP 安全网关外部 IP 地址。在 IPv6 环境中，此属性也可以设为 PCoIP 安全网关的 FQDN。该属性只在安装安全服务器的操作系统为 Windows Server 2008 R2 或更高版本时才可用。 例如：`VDM_SERVER_SS_PCOIP_IPADDR=10.20.30.40` 如果您打算使用 PCoIP 安全网关组件，此属性为必要属性。	无
VDM_SERVER_SS_PCOIP_TCPPORT	PCoIP 安全网关外部 TCP 端口号。该属性只在安装安全服务器的操作系统为 Windows Server 2008 R2 或更高版本时才可用。 例如：`VDM_SERVER_SS_PCOIP_TCPPORT=4172` 如果您打算使用 PCoIP 安全网关组件，此属性为必要属性。	无
VDM_SERVER_SS_PCOIP_UDPPORT	PCoIP 安全网关外部 UDP 端口号。该属性只在安装安全服务器的操作系统为 Windows Server 2008 R2 或更高版本时才可用。 例如：`VDM_SERVER_SS_PCOIP_UDPPORT=4172` 如果您打算使用 PCoIP 安全网关组件，此属性为必要属性。	无

表 7-3. 静默安装安全服务器的 MSI 属性（续）

MSI 属性	说明	默认值
VDM_SERVER_SS_BSG_EXTURL	Blast 安全网关外部 URL。URL 必须包含 HTTPS 协议、可外部解析的安全服务器名和端口号 例如： `VDM_SERVER_SS_BSG_EXTURL=https://view.companydomain.com:8443` 默认端口号为 8443。必须在安全服务器上安装 Blast 安全网关，以允许用户建立与 Horizon 7 桌面的 Web 连接。	无
VDM_SERVER_SS_FORCE_IPSEC	强制在安全服务器和与其配对的连接服务器实例之间使用 IPsec。 默认情况下，在禁用了 IPsec 的情况下执行安全服务器的无人参与安装并将其与连接服务器实例配对时，会导致配对失败。 默认值 1 表示强制使用 IPsec 进行配对。将此值设为 0 则允许不使用 IPsec 进行配对。	1
VDM_IP_PROTOCOL_USAGE	指定 Horizon 7 组件用于通信的 IP 版本。可能的值为 **IPv4** 和 **IPv6**	**IPv4**
VDM_FIPS_ENABLED	指定启用还是禁用 FIPS 模式。值为 1 将启用 FIPS 模式。值为 0 将禁用 FIPS 模式。如果此属性设置为 1 并且 Windows 未处于 FIPS 模式中，则安装程序将中止。	0

移除安全服务器的 IPsec 规则

您必须先移除当前管理安全服务器与其配对的连接服务器实例之间通信的 IPsec 规则，然后才能升级或重新安装安全服务器实例。否则，升级或重新安装将会失败。

默认情况下，安全服务器与其配对的连接服务器实例之间的通信由 IPsec 规则来管理。当您升级或重新安装安全服务器并重新将其与连接服务器实例配对时，必须建立一组新的 IPsec 规则。如果在升级或重新安装前未移除现有 IPsec 规则，则配对会失败。

当您升级或重新安装安全服务器并使用 IPsec 保护安全服务器与连接服务器之间的通信时，必须执行此步骤。

您可以配置一个不使用 IPsec 规则的初始安全服务器配对。安装安全服务器之前，您可以打开 Horizon Administrator 并取消选择默认已启用的全局设置**使用 IPSec 进行安全服务器连接**。如果 IPsec 规则不起作用，则无需在升级或重新安装前移除它们。

注　在升级或重新安装安全服务器之前无需从 Horizon Administrator 中移除安全服务器。只有在您希望将安全服务器从 Horizon 7 环境中永久移除时，才需要将其从 Horizon Administrator 中移除。

在 View 5.0.x 及更低版本中，您可以从 Horizon Administrator 用户界面中移除安全服务器，也可以使用 `vdmadmin -S` 命令行命令移除。对于 View 5.1 及更高版本，则必须使用 `vdmadmin -S`。请参阅《Horizon 7 管理指南》文档中的“使用 -S 选项移除 Horizon 连接服务器实例或安全服务器条目”。

小心　如果移除活动安全服务器的 IPsec 规则，则与安全服务器的所有通信都将丢失，直至您升级或重新安装安全服务器。因此，如果使用负载平衡器管理一组安全服务器，请在一个服务器上执行该过程并升级该服务器，然后再移除下一个服务器的 IPsec 规则。您可以从生产中移除服务器，然后按照这种方式逐个重新添加这些服务器以避免需要为最终用户执行停机。

步骤

1 在 Horizon Administrator 中，单击 **View 配置 > 服务器**。

2 在**安全服务器**选项卡中，选择一个安全服务器，然后单击**更多命令 > 准备升级或重新安装**。

如果在安装安全服务器之前禁用了 IPsec 规则，则该设置无效。这种情况下，您无需在重新安装或升级前移除 IPsec 规则。

3 单击**确定**。

IPsec 规则将被移除，而**准备升级或重新安装**设置将变为无效，指示您可以重新安装或升级安全服务器。

后续步骤

升级或重新安装安全服务器。

Unified Access Gateway 设备优于 VPN 的方面

Unified Access Gateway 设备是从企业防火墙之外对远程桌面和应用程序进行安全访问的默认网关。

有关 Unified Access Gateway 最新版本的文档，请参阅 https://docs.vmware.com/cn/Unified-Access-Gateway/index.html 中的《部署和配置 VMware Unified Access Gateway》文档。

Unified Access Gateway 设备位于网络隔离区 (Demilitarized Zone, DMZ) 中，并作为可信网络内部的连接的代理主机，能够保护虚拟桌面、应用程序主机和服务器免受公共 Internet 的威胁，从而提供额外的安全保护层。

配置 Unified Access Gateway 设备

Unified Access Gateway 与常规 VPN 解决方案类似，因为它们都确保仅将经过严格身份验证的用户产生的流量转发到内部网络。

Unified Access Gateway 优于常规 VPN 的方面包括。

- 访问控制管理器。Unified Access Gateway 自动应用访问规则。Unified Access Gateway 可识别进行内部连接所需的用户授权和寻址。VPN 同样如此，因为大部分 VPN 允许管理员为每个用户或用户组单独配置网络连接规则。一开始，使用 VPN 没有什么问题，但需要投入大量的管理工作以维护所需的规则。
- 用户界面。Unified Access Gateway 并未改变简单直观的 Horizon Client 用户界面。通过使用 Unified Access Gateway，在启动 Horizon Client 时，经过身份验证的用户位于其 View 环境中，并且可以控制对其桌面和应用程序的访问。在启动 Horizon Client 之前，VPN 要求必须先设置 VPN 软件并单独进行身份验证。
- 性能。Unified Access Gateway 从设计上最大限度提高安全性和性能。在 Unified Access Gateway 中，可以保证 PCoIP、HTML Access 和 WebSocket 协议的安全性，无需进行额外封装。VPN 作为 SSL VPN 来实施。该实现满足安全要求，在启用传输层安全 (Transport Layer Security, TLS) 的情况下被视为是安全的，但具有 SSL/TLS 的基础协议仅基于 TCP。现代的视频远程协议利用基于 UDP 的无连接传输，强制使用基于 TCP 的传输时，性能优势将受到极大影响。这并不适用于所有 VPN 技术，因为那些也可以使用 DTLS 或 IPsec 而不是 SSL/TLS 的 VPN 技术可以正确使用 Horizon 7 桌面协议。

使用 Unified Access Gateway 提高 Horizon 安全性

Unified Access Gateway 设备在用户身份验证上面添加设备认证身份验证层以仅限从已知正确的设备中进行访问，并在虚拟桌面基础架构上添加了另一层安全保护，从而提高了安全性。

注 仅在适用于 Windows 的 Horizon Client 上支持该功能。

- 请参阅《部署和配置 VMware Unified Access Gateway》文档中的“在 Unified Access Gateway 设备上配置证书或智能卡身份验证”，网址为 https://docs.vmware.com/cn/Unified-Access-Gateway/index.html。
- 端点合规性检查功能除了提供 Unified Access Gateway 中可用的其他用户身份验证服务之外，还为访问 Horizon 桌面提供了一层额外的安全保护。请参阅 https://docs.vmware.com/cn/Unified-Access-Gateway/index.html 中《部署和配置 VMware Unified Access Gateway》文档的“Horizon 的端点合规性检查”。

重要 如果 Unified Access Gateway 设备配置为双因素身份验证（RSA SecureID 和 RADIUS），启用了 Windows 用户名匹配并具有多个用户域，则应该启用连接服务器以发送域列表，以便用户在使用 Windows 用户名和密码进行身份验证时可以选择正确的域。

双跃点 DMZ

如果在 Internet 和内部网络之间需要使用双跃点 DMZ，您可以将外部 DMZ 中的 Unified Access Gateway 设备部署为内部 DMZ 中的 Unified Access Gateway 的 Web 反向代理以创建双跃点 DMZ 配置。流量可通过每个 DMZ 层中的特定反向代理，但无法绕过 DMZ 层。有关配置详细信息，请参阅《部署和配置 VMware Unified Access Gateway》文档。

Horizon 连接服务器的防火墙规则

必须在防火墙上为连接服务器实例和安全服务器打开某些端口。

安装连接服务器时，安装程序可为您配置所需的 Windows 防火墙规则（可选）。这些规则会打开默认使用的端口。如果在安装后更改了默认端口，则必须手动配置 Windows 防火墙以允许 Horizon Client 设备通过更新的端口连接至 Horizon 7。

下表列出了安装期间可以自动打开的默认端口。如非特别注明，端口均为传入端口。

表 7-4. 在 Horizon 连接服务器安装期间打开的端口

协议	端口	Horizon 连接服务器实例类型
JMS	TCP 4001	标准和副本
JMS	TCP 4002	标准和副本
JMSIR	TCP 4100	标准和副本
JMSIR	TCP 4101	标准和副本
AJP13	TCP 8009	标准和副本
HTTP	TCP 80	标准、副本和安全服务器

表 7-4. 在 Horizon 连接服务器安装期间打开的端口（续）

协议	端口	Horizon 连接服务器实例类型
HTTPS	TCP 443	标准、副本和安全服务器
PCoIP	TCP 4172 传入； UDP 4172 双向传送	标准、副本和安全服务器
HTTPS	TCP 8443 UDP 8443	标准、副本和安全服务器。 在建立到 Horizon 7 的初始连接后，Web 浏览器或客户端设备通过 TCP 端口 8443 连接到 Blast 安全网关。必须在安全服务器或 View 连接服务器实例上启用 Blast 安全网关以允许建立该第二个连接。
HTTPS	TCP 8472	标准和副本 对于 Cloud Pod 架构 功能：用于容器间通信。
HTTP	TCP 22389	标准和副本 对于 Cloud Pod 架构 功能：用于全局 LDAP 复制。
HTTPS	TCP 22636	标准和副本 对于 Cloud Pod 架构 功能：用于安全的全局 LDAP 复制。

配置后端防火墙以支持 IPsec

如果您的网络拓扑在安全服务器与连接服务器实例之间包含后端防火墙，则必须在防火墙上配置某些协议和端口以支持 IPsec。如果配置不正确，则在安全服务器与连接服务器实例之间发送的数据将无法通过防火墙。

默认情况下，IPsec 规则将管理安全服务器与连接服务器实例之间的连接。要支持 IPsec，连接服务器安装程序可在装有 Horizon 7 Server 的 Windows Server 主机上配置 Windows 防火墙规则。对于后端防火墙，您必须自行配置这些规则。

注　强烈建议您使用 IPsec。作为备用方案，您可以禁用 Horizon Administrator 全局设置**使用 IPsec 进行安全服务器连接**。

下列规则必须允许双向流量。您可能要为防火墙上的出入站流量分别指定规则。

需要为使用网络地址转换 (NAT) 和不使用 NAT 的防火墙应用不同的规则。

表 7-5. 支持 IPsec 规则的非 NAT 防火墙要求

源	协议	端口	目标	说明
安全服务器	ISAKMP	UDP 500	Horizon 连接服务器	安全服务器使用 UDP 端口 500 协商 IPsec 安全。
安全服务器	ESP	N/A	Horizon 连接服务器	ESP 协议封装了 IPsec 加密流量。 规则不要求您为 ESP 指定端口。如果需要， 您可指定源和目标 IP 地址 以缩小规则的范围。

以下规则适用于使用 NAT 的防火墙。

表 7-6. 支持 IPsec 规则的 NAT 防火墙要求

源	协议	端口	目标	说明
安全服务器	ISAKMP	UDP 500	Horizon 连接服务器	安全服务器使用 UDP 端口 500 启动 IPsec 安全 协商。
安全服务器	NAT-T ISAKMP	UDP 4500	Horizon 连接服务器	安全服务器使用 UDP 端口 4500 遍历 NAT 和协商 IPsec 安全。

使用备份配置重新安装 Horizon 连接服务器

在某些情况下，您可能需要重新安装当前版本的连接服务器实例，并通过导入包含 View LDAP 配置数据的备份 LDIF 文件来还原现有的 Horizon 7 配置。

例如，作为业务连续性和灾难恢复 (BC/DR) 计划的一部分，您可能需要一套预防措施以防数据中心出现故障。此类计划的第一步是确保在另一位置备份 View LDAP 配置。第二步是在新位置安装连接服务器并导入备份配置，如以下步骤中所述。

在使用现有 Horizon 7 配置来设置其他数据中心时，也可能用到此步骤。或者当您的 Horizon 7 部署仅包含单个连接服务器实例，且该服务器出现问题时，亦有可能用到。

如果副本组中有多个连接服务器实例，当其中单个实例出现故障时，无需执行此步骤。您只需将连接服务器作为副本实例重新进行安装即可。在安装过程中，您需要提供其他连接服务器实例的连接信息，Horizon 7 即会从其他实例还原 View LDAP 配置。

前提条件

- 确认已将 View LDAP 配置备份到加密的 LDIF 文件中。
- 熟悉如何使用 `vdmimport` 命令从 LDIF 备份文件还原 View LDAP 配置。

  请参阅《Horizon 7 管理指南》文档中的“备份和还原 Horizon 7 配置数据”。
- 熟悉新连接服务器实例的安装步骤。请参阅使用新配置安装 Horizon 连接服务器。

步骤

1 使用新配置安装连接服务器。

2 解密已加密的 LDIF 文件。

  例如：

```
vdmimport –d –p mypassword
–f MyEncryptedexport.LDF > MyDecryptedexport.LDF
```

3 导入解密的 LDIF 文件还原 View LDAP 配置。

  例如：

```
vdmimport –f MyDecryptedexport.LDF
```

  注 在此阶段，Horizon 7 配置尚无法访问。客户端无法访问连接服务器或连接到其桌面。

4 使用 Windows 的**添加/删除程序**实用程序从计算机中卸载连接服务器。

请勿卸载称为 AD LDS Instance VMwareVDMDS 实例的 View LDAP 配置。您可以使用**添加/删除程序**实用程序确认 AD LDS Instance VMwareVDMDS 实例未从 Windows Server 计算机中移除。

5 重新安装连接服务器。

根据安装程序的提示接受现有 View LDAP 目录。

后续步骤

使用新配置安装连接服务器实例后，按照您希望的方式来配置连接服务器和 Horizon 7 环境。

Microsoft Windows Installer 命令行选项

要以静默方式安装 Horizon 7 组件，您必须使用 Microsoft Windows Installer (MSI) 命令行选项和属性。Horizon 7 组件安装程序是 MSI 程序，使用标准的 MSI 功能。

有关 MSI 的详细信息，请参阅 Microsoft 网站。有关 MSI 命令行选项，请访问 Microsoft Developer Network (MSDN) 资源库网站，搜索 MSI 命令行选项。要了解 MSI 命令行的用法，可以在安装了 Horizon 7 组件的计算机中打开一个命令提示符，并键入 `msiexec /?`。

要以静默方式运行 Horizon 7 组件安装程序，应当首先静默引导程序，因为该程序会将安装程序提取到一个临时目录中并启动交互式安装。

在命令行中，您必须输入控制安装程序的引导程序的命令行选项。

表 7-7. Horizon 7 组件引导程序的命令行选项

选项	说明
`/s`	禁用引导程序初始屏幕和提取对话框，可阻止显示交互式对话框。 例如：`VMware-viewconnectionserver-y.y.y-xxxxxx.exe /s` 运行静默安装需要 `/s` 选项。
`/v" MSI 命令行选项"`	指示安装程序将您在命令行中输入的双引号括住的字符串作为一组选项进行传递，供 MSI 解析。您必须用双引号括住命令行条目。在 `/v` 之后和命令行末尾之间添加双引号。 例如：`VMware-viewagent-y.y.y-xxxxxx.exe /s /v"command_line_options"` 要指示 MSI 安装程序解释一个包含空格的字符串，应当将该字符串括在两组双引号中。例如，您可能需要将 Horizon 7 组件安装在名称含有空格的安装路径中。 例如：`VMware-viewconnectionserver-y.y.y-xxxxxx.exe /s /v"command_line_options INSTALLDIR=""d:\abc\my folder"""` 在此示例中，MSI 安装程序会传递安装目录的路径，而不会试图将该字符串解释为两个命令行选项。请注意，最后一个双引号的作用是将整个命令行括住。 运行静默安装需要 `/v"命令行选项"` 选项。

您通过将命令行选项和 MSI 属性值传递到 MSI 安装程序 `msiexec.exe` 来控制静默安装的剩余部分。MSI 安装程序中包含 Horizon 7 组件的安装代码。安装程序使用您在命令行中输入的值和选项来解释特定于 Horizon 7 组件的安装选择和设置选项。

表 7-8. MSI 命令行选项和 MSI 属性

MSI 选项或属性	说明
/qn	指示 MSI 安装程序不显示安装程序向导页面。 例如，您可能希望只采用默认的安装选项和功能，以静默方式安装 Horizon Agent： VMware-viewagent-*y.y.y-xxxxxx*.exe /s /v"/qn" 或者，您可以使用 /qb 选项显示非交互式自动安装中的基本进度对话框。 运行静默安装需要 /qn 或 /qb 选项。 有关其他 /q 参数的信息，请访问 Microsoft 开发人员中心网站。
INSTALLDIR	指定 Horizon 7 组件的备用安装路径。 采用*安装目录*=*路径*格式来指定安装路径。如果您要将 Horizon 7 组件安装在默认路径中，则可以忽略此 MSI 属性。 此 MSI 属性是可选的。
ADDLOCAL	确定要安装的特定于组件的选项。 在交互式安装中，Horizon 7 安装程序会显示您可以选择或取消选择的自定义安装选项。在静默安装中，通过在命令行上指定选项，您可以使用 ADDLOCAL 属性选择性地安装各个安装选项。您没有明确指定的选项则不安装。 在交互式安装和静默安装中，Horizon 7 安装程序都将自动安装特定功能。无法使用 ADDLOCAL 控制是否安装这些非可选功能。 键入 ADDLOCAL=ALL 以安装在交互式安装期间可安装的所有自定义安装选项，包括默认安装的选项以及必须选择安装的选项，但 NGVC 除外。NGVC 和 SVIAgent 是相互排斥的。 以下示例将安装 Core、BlastProtocol、PCoIP、UnityTouch、VmVideo、PSG 以及在客户机操作系统上受支持的所有功能：VMware-viewagent-*y.y.y-xxxxxx*.exe /s /v"/qn ADDLOCAL=ALL" 如果您没有使用 ADDLOCAL 属性，将安装默认安装的自定义安装选项以及自动安装的功能。不会安装默认关闭（未选中）的自定义安装选项。 以下示例将安装 Core、BlastProtocol、PCoIP、UnityTouch、VmVideo、PSG 以及在客户机操作系统上受支持且默认开启的自定义安装选项：VMware-viewagent-*y.y.y-xxxxxx*.exe /s /v"/qn" 要单独指定各个安装选项，可键入以逗号分隔的安装选项名称列表。名称之间不要使用空格。采用以下格式：ADDLOCAL=*值,值,值...*。 使用 ADDLOCAL=*value,value,value...* 属性时，您必须包含 Core。 以下示例将安装 Horizon Agent 以及 Core、BlastProtocol、PCoIP、UnityTouch、VmVideo、PSG、Instant Clone Agent 和虚拟打印功能： VMware-viewagent-*y.y.y-xxxxxx*.exe /s /v"/qn ADDLOCAL=Core,NGVC,ThinPrint" 前一示例未安装其他组件，甚至未安装以交互方式默认安装的组件。 ADDLOCAL MSI 属性为可选项。
REBOOT	您可以使用 REBOOT=ReallySuppress 选项，以允许在系统重新引导前完成系统配置任务。 此 MSI 属性是可选的。
/l*v *log_file*	使用详细输出模式将日志记录信息写入指定的日志文件。 例如：/l*v ""%TEMP%\vmmsi.log"" 本示例生成了详细的日志文件，与交互式安装过程中生成的日志类似。 您可以使用该选项记录您安装的专有的自定义功能。您可以使用记录的信息指定在以后的静默安装中需要安装的功能。 /l*v 选项是可选的。

使用 MSI 命令行选项静默卸载 Horizon 7 组件

您可以使用 Microsoft Windows Installer (MSI) 命令行选项卸载 Horizon 7 组件。

语法

```
msiexec.exe
/qb
/x
product_code
```

选项

/qb 选项用于显示卸载进度条。要取消显示卸载进度条，请将 /qb 选项替换为 /qn 选项。

/x 选项用于卸载 Horizon 7 组件。

product_code 字符串用于向 MSI 卸载程序标识 Horizon 7 组件产品文件。您可以在安装时创建的 %TEMP%\vmmsi.log 文件中搜索 ProductCode 以找到*产品代码*字符串。要查找适用于较旧版本 Horizon 7 组件的 *product_code* 字符串，请参阅位于 http://kb.vmware.com/kb/2064845 的 VMware 知识库 (KB) 文章。

关于 MSI 命令行选项的信息，请参阅 Microsoft Windows Installer 命令行选项。

卸载 Horizon Agent 示例

要卸载 32 位 Horizon Agent 版本 7.0.2，请输入以下命令：

```
msiexec.exe /qb /x {B23352D8-AD44-4379-A56E-0E337F9C4036}
```

要卸载 64 位 Horizon Agent 版本 7.0.2，请输入以下命令：

```
msiexec.exe /qb /x {53D6EE37-6B10-4963-81B1-8E2972A1DA4D}
```

在命令中添加详细日志。

```
/l*v "%TEMP%\vmmsi_uninstall.log"
```

如果未明确传递 /l 选项，则默认详细日志文件为 %TEMP%\MSI*nnnn*.log，其中 *nnnn* 是四字符 GUID。

Horizon Agent 卸载进程会保留某些注册表项。需要使用这些注册表项，才能保留相应的连接服务器配置信息，以使远程桌面即使在卸载代理并重新安装之后，仍能够继续与连接服务器配对。移除这些注册表项将会破坏配对。

需保留以下注册表项：

- HKLM\SOFTWARE\Microsoft\SystemCertificates\VMware Horizon View Certificates*
- HKLM\SOFTWARE\Microsoft\SystemCertificates\VMwareView\Certificates*
- HKLM\SOFTWARE\Microsoft\SystemCertificates\VMwareView\CRLs
- HKLM\SOFTWARE\Microsoft\SystemCertificates\VMwareView\CTLs
- HKLM\SOFTWARE\Policies\VMware, Inc.\VMware VDM*

- HKLM\SOFTWARE\Policies\VMware, Inc.\vRealize Operations for Horizon*
- HKLM\SOFTWARE\VMware, Inc.\VMware VDM*
- HKLM\SOFTWARE\Wow6432Node\Microsoft\SystemCertificates\VMware Horizon View Certificates*
- HKLM\SOFTWARE\Wow6432Node\Microsoft\SystemCertificates\VMwareView*
- HKLM\SOFTWARE\Wow6432Node\Policies\VMware, Inc.\VMware VDM*
- HKLM\SOFTWARE\Wow6432Node\Policies\VMware, Inc.\vRealize Operations for Horizon*
- HKLM\SOFTWARE\Wow6432Node\VMware, Inc.
- HKLM\SOFTWARE\Wow6432Node\VMware, Inc.\VMware VDM

为 Horizon 7 Server 配置 TLS 证书

8

VMware 强烈建议您为连接服务器实例、安全服务器和 View Composer 服务实例配置 TLS 证书以进行身份验证。

安装连接服务器实例、安全服务器或 View Composer 实例时，会生成一个默认的 TLS 服务器证书。您可以使用默认证书来进行测试。

用于连接服务器之间以及 Horizon Agent 和连接服务器实例之间通信的证书通过一种自动机制来进行替换，而无法手动替换。有关更多详细信息，请参见《Horizon 7 安全指南》文档。

重要 应尽快替换默认证书。默认证书不是由证书颁发机构 (CA) 签发的。如果使用未经 CA 签发的证书，不受信任的第三方将有可能伪装成您的服务器并截获流量。

本章讨论了以下主题：

- 了解 Horizon 7 Server 的 TLS 证书
- TLS 证书设置任务概述
- 获取 CA 签发的 TLS 证书
- 配置 Horizon 连接服务器、安全服务器或 View Composer 以使用新 TLS 证书
- 配置客户端端点以信任根证书和中间证书
- 为服务器证书配置证书撤消检查
- 配置 PCoIP 安全网关以使用新 TLS 证书
- 将 Horizon Administrator 设置为信任 vCenter Server 或 View Composer 证书
- 使用 CA 签发的 TLS 证书的优势
- Horizon 连接服务器和安全服务器上的证书问题故障排除

了解 Horizon 7 Server 的 TLS 证书

在为 Horizon 7 Server 及相关组件配置 TLS 证书时必须遵循特定的指导原则。

Horizon 连接服务器和安全服务器

客户端与服务器之间的连接需要使用 TLS。面向客户端的连接服务器实例、安全服务器和用于终止 TLS 连接的中间服务器都需要 TLS 服务器证书。

默认情况下，在安装连接服务器或安全服务器时，安装程序会为服务器生成一个自签名证书。但在以下情况中，安装程序仍使用现有证书：

- 如果 Windows 证书存储区中已存在友好名称为 vdm 的有效证书
- 如果您从较早版本升级到 Horizon 7，且在 Windows Server 计算机上配置了有效的密钥存储文件，则安装会提取密钥和证书，并将其导入到 Windows 证书存储区中。

vCenter Server 和 View Composer

在生产环境的 Horizon 7 中添加 vCenter Server 和 View Composer 之前，请确保 vCenter Server 和 View Composer 使用由 CA 签发的证书。

有关替换 vCenter Server 默认证书的信息，请参阅 VMware 技术白皮书站点 (http://www.vmware.com/resources/techresources/) 中的“替换 vCenter Server 证书”。

如果您在同一 Windows Server 主机上安装 vCenter Server 和 View Composer，它们可以使用相同的 TLS 证书，但必须单独为每个组件配置证书。

PCoIP 安全网关

为了遵循行业或司法辖区的安全规定，您可将 PCoIP 安全网关 (PCoIP Secure Gateway, PSG) 服务生成的默认 TLS 证书替换成 CA 签发的证书。我们强烈建议配置 PSG 服务使用 CA 签发的证书，特别是对于需要使用安全扫描程序通过合规性测试的部署。请参阅 配置 PCoIP 安全网关以使用新 TLS 证书。

Blast 安全网关

默认情况下，Blast 安全网关 (Blast Secure Gateway, BSG) 将使用为运行 BSG 的连接服务器实例或安全服务器配置的 TLS 证书。如果您将服务器的默认自签名证书替换为 CA 签发的证书，则 BSG 也会使用 CA 签发的证书。

SAML 2.0 身份验证器

VMware Identity Manager 使用 SAML 2.0 身份验证器为不同的安全域提供基于 Web 的身份验证和授权。如果希望 Horizon 7 将身份验证委派给 VMware Identity Manager，可以将 Horizon 7 配置为接受经过 SAML 2.0 身份验证的 VMware Identity Manager 会话。当 VMware Identity Manager 被配置为支持 Horizon 7 时，VMware Identity Manager 用户可以通过选择 Horizon 用户门户上的桌面图标连接至远程桌面。

在 Horizon Administrator 中，您可以配置 SAML 2.0 身份验证器，以将其与连接服务器实例配合使用。

在 Horizon Administrator 中添加 SAML 2.0 身份验证器之前，请确保 SAML 2.0 身份验证器使用 CA 签发的证书。

其他指导原则

有关请求和使用 CA 签发的 TLS 证书的一般信息，请参阅 使用 CA 签发的 TLS 证书的优势。

当客户端端点连接到连接服务器实例或安全服务器时，系统会向它们显示相应服务器的 TLS 服务器证书和信任链中的任何中间证书。要信任服务器证书，客户端系统必须已安装签发 CA 的根证书。

当连接服务器与 vCenter Server 和 View Composer 通信时，系统会向连接服务器显示 TLS 服务器证书和这些服务器的中间证书。要信任 vCenter Server 和 View Composer Server，连接服务器计算机必须已安装签发 CA 的根证书。

同样，如果为连接服务器配置了 SAML 2.0 身份验证器，则连接服务器计算机必须已为 SAML 2.0 服务器证书安装签发 CA 的根证书。

TLS 证书设置任务概述

要为 Horizon 7 Server 设置 TLS 服务器证书，必须执行多项高级任务。

在连接服务器副本实例容器中，您必须对容器中的所有实例执行这些任务。

执行这些任务的步骤在本概述随后的主题中有具体介绍。

1 确定是否需要从 CA 获取新的 TLS 签名证书。

  如果贵组织已经拥有有效的 TLS 服务器证书，您可以使用该证书替换随连接服务器、安全服务器或 View Composer 提供的默认 TLS 服务器证书。要使用现有证书，您还需要用到附带的私钥。

出发点	操作
您的组织为您提供了一个有效的 TLS 服务器证书。	直接转至步骤 2。
您没有 TLS 服务器证书。	从 CA 获取签发的 TLS 服务器证书。

2 将 TLS 证书导入 Horizon 7 Server 主机上的 Windows 本地计算机证书存储区。

3 对于连接服务器实例和安全服务器，请将证书的友好名称修改为 **vdm**。

  只能为每个 Horizon 7 Server 主机上的一个证书分配友好名称 **vdm**。

4 在连接服务器计算机上，如果根证书不受 Windows Server 主机信任，请将根证书导入 Windows 本地计算机证书存储区。

  此外，如果连接服务器实例不信任为安全服务器、View Composer 和 vCenter Server 主机配置的 TLS 服务器证书的根证书，也必须导入这些根证书。应仅对连接服务器实例执行这些步骤。您无需将根证书导入 View Composer、vCenter Server 或安全服务器主机。

5 如果您的服务器证书由中间 CA 签发，请将中间证书导入 Windows 本地计算机证书存储区。

  要简化客户端配置，请将整个证书链导入 Windows 本地计算机证书存储区。如果 Horizon 7 Server 缺少中间证书，则必须为客户端和启动 Horizon Administrator 的计算机配置这些中间证书。

6 对于 View Composer 实例，请执行以下步骤之一：

  - 如果在安装 View Composer 前将证书导入 Windows 本地计算机证书存储区，则可以在安装 View Composer 过程中选择您的证书。
  - 如果在安装 View Composer 后想使用新证书替换现有证书或默认的自签名证书，必须运行 `SviConfig ReplaceCertificate` 实用程序，以将新证书与 View Composer 使用的端口绑定。

7 如果您的 CA 不是公认 CA，请对客户端进行配置，使其信任根证书和中间证书。

  另外还需要确保启动 Horizon Administrator 的计算机信任根证书和中间证书。

8 确定是否要重新配置证书撤消检查。

连接服务器会针对 Horizon 7 Server、View Composer 和 vCenter Server 执行证书撤消检查。CA 签发的大多数证书都包含证书撤消信息。如果您的 CA 不包含此信息，则可以对服务器进行配置，使其不执行证书撤消检查。

如果配置了 SAML 身份验证器以用于连接服务器实例，连接服务器也会对 SAML 服务器证书执行证书撤消检查。

获取 CA 签发的 TLS 证书

如果贵组织未提供 TLS 服务器证书，则您必须请求由 CA 签发的新证书。

您可以通过多种方法获取新的签名证书。例如，您可以使用 Microsoft `certreq` 实用程序生成证书签发请求 (CSR) 并提交至 CA。

有关如何使用 `certreq` 来完成此任务的信息，请参阅《为 Horizon 7 设置 TLS 证书的方案》文档中的示例。

出于测试目的，您可以基于不受信任的根从许多 CA 获取免费的临时证书。

重要 从 CA 获取 TLS 签名证书时，必须遵循特定的规则和准则。

- 在计算机上生成证书请求时，请确保同时生成一个私钥。获取 TLS 服务器证书并将其导入 Windows 本地计算机证书存储区时，必须有一个与证书对应的附带私钥。
- 为了遵循 VMware 安全建议，请使用客户端设备在连接主机时使用的完全限定域名 (FQDN)。不要使用简单的服务器名称或 IP 地址，即使内部域中的通信也是如此。
- 请勿使用仅与 Windows Server 2008 企业 CA 或更高版本兼容的证书模板为服务器创建证书。
- 请勿使用小于 1024 的 `KeyLength` 值为服务器生成证书。客户端终端无法验证服务器上生成的 `KeyLength` 小于 1024 的证书，继而客户端将无法连接到服务器。连接服务器执行的证书验证也会失败，进而导致受影响的服务器在 Horizon Administrator 控制板中显示为红色。

有关获取证书的一般信息，请查询 MMC 证书插件中提供的 Microsoft 联机帮助。如果您的计算机上未安装证书插件，请参阅将证书管理单元添加到 MMC。

获取 Windows 域或企业 CA 签发的证书

要从 Windows 域或企业 CA 获取签发证书，可以使用 Windows 证书存储区中的 Windows 证书注册向导。

如果计算机之间的通信保持在您的内部域中，则此请求证书的方法很适用。例如，从 Windows 域 CA 获取签发证书可能适用于服务器之间的通信。

如果您的客户端从外部网络连接到 Horizon 7 Server，则需请求由受信任的第三方 CA 签发的 TLS 服务器证书。

前提条件

- 确定客户端设备在连接主机时使用的完全限定域名 (FQDN)。

  为了遵循 VMware 安全建议，请使用 FQDN 而不是简单的服务器名称或 IP 地址，即使内部域中的通信也是如此。

- 确认证书插件已添加至 MMC。请参阅将证书管理单元添加到 MMC。
- 确认您具有相应的凭据以请求可颁发给计算机或服务的证书。

步骤

1 在 Windows Server 主机上的 **MMC** 窗口中，展开**证书 (本地计算机)** 节点并选择**个人**文件夹。

2 从**操作**菜单中，转到**所有任务 > 请求新证书**以显示**证书注册**向导。

3 选择证书注册策略。

4 选择要请求的证书的类型，选择**使私钥可以导出**选项，然后单击**注册**。

5 单击**完成**。

新签发的证书将添加到 Windows 证书存储区内的**个人 > 证书**文件夹。

后续步骤

- 确认服务器证书和证书链已导入到 Windows 证书存储区中。
- 对于连接服务器实例或安全服务器，请将证书的友好名称修改为 **vdm**。请参阅修改证书的友好名称。
- 对于 View Composer Server，将新证书与 View Composer 使用的端口绑定。请参阅 将新 TLS 证书绑定至 View Composer 使用的端口。

配置 Horizon 连接服务器、安全服务器或 View Composer 以使用新 TLS 证书

要将连接服务器实例、安全服务器或 View Composer 实例配置为使用 TLS 证书，必须将服务器证书和整个证书链导入连接服务器、安全服务器或 View Composer 主机上的 Windows 本地计算机证书存储区中。

在连接服务器副本实例容器中，您必须在容器中的所有实例上导入服务器证书和证书链。

默认情况下，Blast 安全网关 (BSG) 将使用为运行 BSG 的连接服务器实例或安全服务器配置的 TLS 证书。如果您将 View server 的默认自签名证书替换为 CA 签发的证书，则 BSG 也会使用 CA 签发的证书。

重要 要将连接服务器或安全服务器配置为使用某个证书，您必须将该证书的友好名称更改为 **vdm**。此外，该证书必须有附带的私钥。

如果在安装 View Composer 后想使用新证书替换现有证书或默认的自签名证书，则必须运行 `SviConfig ReplaceCertificate` 实用程序，以将新证书与 View Composer 使用的端口绑定。

步骤

1 将证书管理单元添加到 MMC

您必须先向装有 Horizon 7 Server 的 Windows Server 主机上的 Microsoft 管理控制台 (MMC) 中添加证书管理单元，然后才能将证书添加到 Windows 证书存储区中。

2 将签名的服务器证书导入到 Windows 证书存储区

您必须将 TLS 服务器证书导入到安装了连接服务器实例或安全服务器服务的 Windows Server 主机上的 Windows 本地计算机证书存储区中。

3 修改证书的友好名称

要将连接服务器实例或安全服务器配置为识别并使用 TLS 证书，必须将证书的友好名称修改为 vdm。

4 将根证书和中间证书导入 Windows 证书存储区

如果安装连接服务器的 Windows Server 主机不信任 TLS 服务器签名证书的根证书，则必须将根证书导入 Windows 本地计算机证书存储区。此外，如果连接服务器主机不信任为安全服务器、View Composer 和 vCenter Server 主机配置的 TLS 服务器证书的根证书，也必须导入这些根证书。

5 将新 TLS 证书绑定至 View Composer 使用的端口

如在安装 View Composer 后配置新的 TLS 证书，则必须运行 `SviConfig ReplaceCertificate` 实用程序以替换绑定至 View Composer 所用端口的证书。该实用程序可解除绑定现有证书，并可将新证书绑定至该端口。

将证书管理单元添加到 MMC

您必须先向装有 Horizon 7 Server 的 Windows Server 主机上的 Microsoft 管理控制台 (MMC) 中添加证书管理单元，然后才能将证书添加到 Windows 证书存储区中。

前提条件

确认装有 Horizon 7 Server 的 Windows Server 计算机上的 MMC 和证书管理单元均可用。

步骤

1 在 Windows Server 计算机中，单击**开始**，然后键入 **mmc.exe**。

2 在 **MMC** 窗口中，转到**文件 > 添加/删除管理单元**。

3 在**添加/删除管理单元**窗口中，选择**证书**，然后单击**添加**。

4 在**证书管理单元**窗口中，选择**计算机帐户**，单击**下一步**，选择**本地计算机**，然后单击**完成**。

5 在**添加或删除管理单元**窗口中，单击**确定**。

后续步骤

将 TLS 服务器证书导入至 Windows 证书存储区中。

将签名的服务器证书导入到 Windows 证书存储区

您必须将 TLS 服务器证书导入到安装了连接服务器实例或安全服务器服务的 Windows Server 主机上的 Windows 本地计算机证书存储区中。

您还必须在安装了 View Composer 服务的 Windows Server 主机上执行此任务。

根据您的证书文件格式，密钥存储文件中的整个证书链可能都会被导入到 Windows 本地计算机证书存储区。例如，可能会导入服务器证书、中间证书和根证书。

对于其他类型的证书文件，只有服务器证书会被导入到 Windows 本地计算机证书存储区。这种情况下，您必须单独导入证书链中的根证书和全部中间证书。

有关证书的更多信息，请参考 MMC 证书插件中提供的 Microsoft 联机帮助。

注　如果要将 TLS 连接分流负载到中间服务器，则必须将同一 TLS 服务器证书同时导入到中间服务器和被分流负载的 Horizon 7 Server。有关详细信息，请参阅《Horizon 7 管理指南》文档中的“将 TLS 连接负载分流到中间服务器”。

前提条件

确认证书插件已添加至 MMC。请参阅将证书管理单元添加到 MMC。

步骤

1 在 Windows Server 主机上的 MMC 窗口中，展开**证书 (本地计算机)** 节点并选择**个人**文件夹。

2 在“操作”窗格中，转到**更多操作 > 所有任务 > 导入**。

3 在**证书导入**向导中，单击**下一步**并浏览至存储证书的位置。

4 选择证书文件并单击**打开**。

要显示您的证书文件类型，可以从**文件名**下拉菜单中选择其文件格式。

5 键入证书文件中所含私钥的密码。

6 选择**将此密钥标记为可导出**。

7 选择**包含所有已扩展属性**。

8 单击**下一步**，然后单击**完成**。

新证书会显示在**证书 (本地计算机) > 个人 > 证书**文件夹中。

9 确认新证书包含私钥。

a 在**证书 (本地计算机) > 个人 > 证书**文件夹中，双击新证书。

b 在“证书信息”对话框的“常规”选项卡中，确认显示有以下语句：您有一个与该证书对应的私钥 (You have a private key that corresponds to this certificate)。

后续步骤

将证书的友好名称修改为 **vdm**。

修改证书的友好名称

要将连接服务器实例或安全服务器配置为识别并使用 TLS 证书，必须将证书的友好名称修改为 vdm。

没有必要修改 View Composer 所使用的 TLS 证书的友好名称。

前提条件

确认已将服务器证书导入到 Windows 证书存储区的**证书 (本地计算机) > 个人 > 证书**文件夹中。请参阅将签名的服务器证书导入到 Windows 证书存储区。

步骤

1 在 Windows Server 主机上的 MMC 窗口中，展开**证书 (本地计算机)** 节点并选择**个人 > 证书**文件夹。

2 右键单击颁发给 Horizon 7 Server 主机的证书，然后单击**属性**。

3 在“常规”选项卡上，删除**友好名称**文本并键入 **vdm**。

4 单击**应用**，然后单击**确定**。

5 确认**个人 > 证书**文件夹中没有其他服务器证书采用友好名称 **vdm**。

   a 查找任何其他服务器证书，右键单击证书，然后单击**属性**。

   b 如果证书的友好名称为 **vdm**，请删除该名称，单击**应用**，然后单击**确定**。

后续步骤

将根证书和中间证书导入到 Windows 本地计算机证书存储区中。

导入证书链中的所有证书后，必须重新启动连接服务器服务或安全服务器服务以使所做的更改生效。

将根证书和中间证书导入 Windows 证书存储区

如果安装连接服务器的 Windows Server 主机不信任 TLS 服务器签名证书的根证书，则必须将根证书导入 Windows 本地计算机证书存储区。此外，如果连接服务器主机不信任为安全服务器、View Composer 和 vCenter Server 主机配置的 TLS 服务器证书的根证书，也必须导入这些根证书。

如果连接服务器、安全服务器、View Composer 和 vCenter Server 证书由连接服务器主机信任的已知根 CA 签发，且您的证书链中没有中间证书，则可以跳过此任务。常用的证书颁发机构都可能受主机信任。

您必须在一个容器中的所有连接服务器副本实例上导入不受信任的根证书。

注 您无需将根证书导入 View Composer、vCenter Server 或安全服务器主机。

如果服务器证书是由中间 CA 签发，还必须导入证书链中的每个中间证书。要简化客户端配置，可将整个中间证书链导入安全服务器、View Composer、vCenter Server 主机以及连接服务器主机。如果连接服务器或安全服务器主机缺少中间证书，则必须为客户端和启动 Horizon Administrator 的计算机配置这些中间证书。如果 View Composer 或 vCenter Server 主机缺少中间证书，则必须为每个连接服务器实例配置这些中间证书。

如果您已确认整个证书链都已导入 Windows 本地计算机证书存储区，则可以跳过此任务。

注 如果配置了 SAML 身份验证器以供连接服务器实例使用，则同样的准则也适用于 SAML 2.0 身份验证器。如果连接服务器主机不信任为 SAML 身份验证器配置的根证书，或者 SAML 服务器证书由中间 CA 签发，则必须确保将证书链导入到 Windows 本地计算机证书存储区中。

步骤

1 在 Windows Server 主机上的 MMC 控制台中，展开**证书 (本地计算机)** 节点并转到**受信任的根证书颁发机构 > 证书**文件夹。

   - 如果您的根证书位于此文件夹，且证书链中没有中间证书，则跳至步骤 7。
   - 如果您的根证书不在此文件夹，则执行步骤 2。

2 右键单击**受信任的根证书颁发机构 > 证书**文件夹，然后单击**所有任务 > 导入**。

3 在**证书导入**向导中，单击**下一步**并浏览至存储根 CA 证书的位置。

4 选择根 CA 证书文件并单击**打开**。

5 连续单击**下一步**，然后单击**完成**。

6 如果您的服务器证书由中间 CA 签发，请将证书链中的所有中间证书导入 Windows 本地计算机证书存储区。

   a 转到**证书 (本地计算机) > 中间证书颁发机构 > 证书**文件夹。

   b 针对每个必须导入的中间证书重复执行步骤 3 到步骤 6。

7 重新启动连接服务器服务、安全服务器服务、View Composer 服务或 vCenter Server 服务，使所做的更改生效。

将新 TLS 证书绑定至 View Composer 使用的端口

如在安装 View Composer 后配置新的 TLS 证书，则必须运行 `SviConfig ReplaceCertificate` 实用程序以替换绑定至 View Composer 所用端口的证书。该实用程序可解除绑定现有证书，并可将新证书绑定至该端口。

如在安装 View Composer 之前在 Windows Server 计算机中安装新证书，则不必运行 `SviConfig ReplaceCertificate` 实用程序。运行 View Composer 安装程序时，你可选择由 CA 签发的某个证书取代默认的自签发证书。安装过程中会将选择的证书绑定至 View Composer 使用的端口。

如您试图将现有证书或默认的自签发证书替换为新证书，则必须使用 `SviConfig ReplaceCertificate` 实用程序。

前提条件

确认已将新证书导入至安装有 View Composer 的 Windows Server 计算机中的 Windows 本地计算机证书存储区中。

步骤

1 停止 View Composer 服务。

2 在安装了 View Composer 的 Windows Server 主机上，打开命令提示符。

3 导航到 `SviConfig` 可执行文件。

   该文件与 View Composer 应用程序位于同一位置。默认路径为 `C:\Program Files (x86)\VMware\VMware View Composer\sviconfig.exe`。

4 键入 SviConfig ReplaceCertificate 命令。

例如：

```
sviconfig –operation=ReplaceCertificate
          –delete=false
```

其中 –delete 是必需的参数，应用于被替换的证书。您必须指定 –delete=true 以从 Windows 本地计算机证书存储区中删除旧证书，或者指定 –delete=false 以保留 Windows 证书存储区中的旧证书。

实用程序显示 Windows 本地计算机证书存储区中可使用的 TLS 证书编号列表。

5 要选择某个证书，请键入证书的编号，并按 Enter。

6 重新启动 View Composer 服务，使所做更改生效。

示例：SviConfig ReplaceCertificate

下例替换了绑定至 View Composer 端口的证书：

```
sviconfig –operation=ReplaceCertificate
          –delete=false
```

配置客户端端点以信任根证书和中间证书

如果 Horizon 7 Server 证书是由访问 Horizon Administrator 的客户端计算机不信任的 CA 签发，您可以配置域中的所有 Windows 客户端系统以信任根证书和中间证书。为此，您必须将根证书的公钥添加到 Active Directory 中的“受信任的根证书颁发机构”组策略，并将根证书添加到 Enterprise NTAuth 存储区。

例如，如果您的组织使用内部证书服务，您可能需要采取下述步骤。

如果 Windows 域控制器充当根 CA，或您的证书由公认的 CA 签名，则无需采取下述步骤。对于众所周知的 CA，操作系统供应商会在客户端系统上预先安装根证书。

如果服务器证书是由一个非公认的中间 CA 签发，则必须将该中间证书添加到 Active Directory 的“中间证书颁发机构”组策略中。

对于使用 Windows 之外的其他操作系统的客户端设备，请参阅以下针对用户可安装的根证书和中间证书的分发说明：

- 对于适用于 Mac 的 Horizon Client，请参阅配置适用于 Mac 的 Horizon Client 以信任根证书和中间证书。
- 对于适用于 iOS 的 Horizon Client，请参阅将适用于 iOS 的 Horizon Client 配置为信任根证书和中间证书。
- 对于适用于 Android 的 Horizon Client，请参阅 Google 网站上的文档，例如，《Android 3.0 用户指南》。
- 对于适用于 Linux 的 Horizon Client，请参阅 Ubuntu 文档

前提条件

确认生成的服务器证书的 KeyLength 值为 1024 或更大值。客户端端点将不对服务器上生成的、KeyLength 值小于 1024 的证书进行验证，客户端将无法连接到服务器。

步骤

1 在 Active Directory 服务器上使用 `certutil` 命令，将证书发布到 Enterprise NTAuth 存储区中。

例如：**`certutil –dspublish –f` *`CA 根证书路径`* `NTAuthCA`**

2 在 Active Directory 服务器上，导航至组策略管理插件。

AD 版本	导航路径
Windows 2003	a 选择**开始 > 所有程序 > 管理工具 > Active Directory 用户和计算机**。 b 右键单击域，然后单击**属性**。 c 在**组策略**选项卡上，单击**打开**以打开组策略管理插件。 d 右键单击**默认域策略**并单击**编辑**。
Windows 2008	a 选择**开始 > 管理工具 > 组策略管理**。 b 展开您的域，右键单击**默认域策略**并单击**编辑**。
Windows 2012 R2	a 选择**开始 > 管理工具 > 组策略管理**。 b 展开您的域，右键单击**默认域策略**并单击**编辑**。
Windows 2016	a 选择**开始 > 管理工具 > 组策略管理**。 b 展开您的域，右键单击**默认域策略**并单击**编辑**。

3 展开**计算机配置**部分，然后转到 **Windows 设置 > 安全性设置 > 公钥策略**。

4 导入证书。

选项	说明
根证书	a 右键单击**受信任的根证书颁发机构**，然后选择**导入**。 b 按照向导中的提示导入根证书（如 `rootCA.cer`）并单击**确定**。
中间证书	a 右键单击**中间证书颁发机构**，然后选择**导入**。 b 按照向导中的提示导入中间证书（如 `intermediateCA.cer`）并单击**确定**。

5 关闭**组策略**窗口。

现在域中所有系统的受信任根证书存储区和中间证书存储区中都已具备证书信息，可以信任根证书和中间证书。

配置适用于 Mac 的 Horizon Client 以信任根证书和中间证书

如果服务器证书是由运行适用于 Mac 的 Horizon Client 计算机不信任的 CA 签名的，您可以配置这些计算机以信任根证书和中间证书。您必须将根证书和信任链中的所有中间证书分发给客户端计算机。

步骤

1 将根证书和中间证书传送到运行适用于 Mac 的 Horizon Client 的计算机。

2 在 Mac 计算机上打开根证书。

该证书显示以下消息：您要电脑从现在开始信任由 *`CA 名称`*签名的证书吗?

3 单击**总是信任**

4 键入用户密码。

5 针对信任链中的所有中间证书重复执行步骤 2 到步骤 4。

将适用于 iOS 的 Horizon Client 配置为信任根证书和中间证书

如果服务器证书是由运行适用于 iOS 的 Horizon Client 的 iPad 和 iPhone 所不信任的 CA 签发，则可以将设备配置为信任根证书和中间证书。您必须将根证书和信任链中的所有中间证书分发到设备。

步骤

1 将根证书和中间证书作为电子邮件附件发送到 iPad。

2 打开电子邮件附件以获取根证书，并选择**安装**。

证书将显示以下消息：

> 配置文件无法验证。无法验证*证书名称*的真实性。安装该配置文件将更改 iPad 上的设置。根证书。安装证书 *Certificate name* 会将其添加到 iPad 上的可信证书列表中。

3 再次选择**安装**。

4 对信任链中的所有中间证书重复步骤 2 和 3。

为服务器证书配置证书撤消检查

每个连接服务器实例都会对自身的证书以及与其配对的安全服务器的证书执行证书撤消检查。同时，每个实例还会在与 vCenter Server 和 View Composer Server 建立连接时检查其证书。默认情况下，证书链中除了根证书之外的所有证书都在检查之列。但您可以更改此默认设置。

如果配置了 SAML 2.0 身份验证器以供连接服务器实例使用，连接服务器也会对 SAML 2.0 服务器证书执行证书撤消检查。

Horizon 7 支持多种证书撤消检查方法，例如，证书撤消列表 (CRL) 和联机证书状态协议 (Online Certificate Status Protocol, OCSP)。CRL 是由颁发证书的 CA 发布的吊销证书列表。OCSP 是一种证书验证协议，用于获取 X.509 证书的撤消状态。

借助 CRL，撤消证书列表会从证书分发点 (DP) 下载，证书中通常都会指定这一分发点。该服务器会定期转到证书中指定的 CRL DP URL 下载列表，并检查以确定是否已撤消了服务器证书。借助 OCSP，该服务器会向 OCSP 响应程序发送请求，以确定证书的撤消状态。

从第三方证书颁发机构 (CA) 获取服务器证书时，证书包含一种或多种可用来确定其撤消状态的方法，例如，CRL DP URL 或 OCSP 响应程序的 URL。如果您有自己的 CA 并生成了证书，但证书中不包含撤消信息，则证书撤消检查会失败。此类证书的撤消信息可能包括：托管 CRL 的服务器上基于 Web 的 CRL DP 的 URL。

如果您有自己的 CA，但证书中没有或不能包含证书撤消信息，则可以选择不检查证书的撤消信息或只检查证书链中的特定证书。在该服务器上，您可以使用 Windows 注册表编辑器在 `HKLM\Software\VMware, Inc.\VMware VDM\Security` 下创建字符串 (REG_SZ) 值 **CertificateRevocationCheckType**，并将其设置为以下数据值之一。

值	说明
1	不执行证书撤消检查。
2	仅检查服务器证书。不检查证书链中的任何其他证书。
3	检查证书链中的所有证书。
4	（默认）检查除根证书之外的所有证书。

如果未设置此注册表值，或设置的值无效（即，值不是 1、2、3 或 4），则除根证书之外的所有证书都在检查之列。在每个您要修改撤消检查的服务器上设置此注册表值。设置此值后，无需重新启动系统。

注　如果贵组织使用代理设置进行 Internet 访问，可能需要将您的连接服务器计算机配置为使用代理设置，以确保能够针对安全服务器或用于客户端安全连接的连接服务器实例执行证书撤消检查。如果连接服务器实例无法访问 Internet，则证书撤消检查可能会失败，并且连接服务器实例或与其配对的安全服务器可能在 Horizon Administrator 控制板中显示为红色。要解决此问题，请参阅《Horizon 7 管理指南》文档中的“排除安全服务器证书撤消检查中的故障”。

配置 PCoIP 安全网关以使用新 TLS 证书

为了遵循行业或司法辖区的安全规定，您可将 PCoIP 安全网关 (PSG) 服务生成的默认 TLS 证书替换成 CA 签发的证书。

在 Horizon 7 中，PSG 服务会在启动时创建默认的自签名 TLS 证书。PSG 服务会将自签名证书提供给运行连接到 PSG 的 Horizon Client 2.0（或适用于 Windows 的 Horizon Client 5.2）或更高版本的客户端。

PSG 还会提供一个默认的旧版 TLS 证书，该证书将提供给运行连接到 PSG 的旧版 View Client 或更早版本的客户端。

默认证书会提供从客户端端点到 PSG 的安全连接，并且不需要在 Horizon Administrator 中进行进一步配置。但是，我们强烈建议配置 PSG 服务使用 CA 签发的证书，特别是对于需要使用安全扫描程序通过合规性测试的部署。

尽管不是强制要求，但是您最好能在将默认 PSG 证书替换成 CA 签发的证书前，为服务器配置 CA 签发的新 TLS 证书。进行下面的步骤前，您应先为运行 PSG 的服务器将 CA 签发的证书导入到 Windows 证书存储区。

注　如果您使用安全扫描程序进行合规性测试，最好先设置 PSG 使用与服务器相同的证书，并在扫描 PSG 端口前先扫描 View 端口。这样一来，您就可以先解决在扫描 View 端口时出现的信任或验证问题，从而避免这些问题造成 PSG 端口和证书测试失效。接下来，您即可为 PSG 配置唯一的证书并进行下一项扫描。

步骤

1　确认服务器名称与 PSG 证书使用者名称相匹配

安装连接服务器实例或安全服务器时，安装程序会创建一个注册表设置，其中的值包含计算机的 FQDN。您必须确认该值与安全扫描程序用于访问 PSG 端口的 URL 的服务器名称部分相匹配。该服务器名称还必须与您希望用于 PSG 的 TLS 证书的使用者名称或使用者替代名称 (SAN) 相匹配。

2 在 Windows 证书存储区中配置 PSG 证书

要将默认的 PSG 证书替换为 CA 签发的证书，必须在运行 PSG 的连接服务器或安全服务器计算机上的 Windows 本地计算机证书存储区中配置证书及其私钥。

3 在 Windows 注册表中设置 PSG 证书友好名称

PSG 会通过服务器名称和证书友好名称识别要使用的 TLS 证书。您必须在运行 PSG 的连接服务器或安全服务器计算机上的 Windows 注册表中设置友好名称值。

4 （可选）与 PSG 连接时强制使用 CA 签发的证书

您可以确保与 PSG 的所有客户端连接均对 PSG 使用 CA 签发的证书，而不是默认的旧版证书。此步骤不是为 PSG 配置 CA 签发证书的必需步骤。只有需要在您的 Horizon 7 部署中强制使用 CA 签发的证书时，才采取这些步骤。

确认服务器名称与 PSG 证书使用者名称相匹配

安装连接服务器实例或安全服务器时，安装程序会创建一个注册表设置，其中的值包含计算机的 FQDN。您必须确认该值与安全扫描程序用于访问 PSG 端口的 URL 的服务器名称部分相匹配。该服务器名称还必须与您希望用于 PSG 的 TLS 证书的使用者名称或使用者替代名称 (SAN) 相匹配。

例如，如果扫描程序通过 URL `https://view.customer.com:4172` 连接 PSG，则注册表设置必须包含 `view.customer.com` 值。请注意，安装过程中设置的连接服务器或安全服务器计算机的 FQDN 可能与此外部服务器名称不同。

步骤

1 在运行 PCoIP 安全网关的连接服务器或安全服务器主机上启动 Windows 注册表编辑器。

2 导航至 `HKEY_LOCAL_MACHINE\SOFTWARE\Teradici\SecurityGateway\SSLCertPsgSni` 注册表设置。

3 确认 `SSLCertPsgSni` 设置的值与扫描程序用于连接 PSG 的 URL 中的服务器名称相匹配，且与您希望为 PSG 安装的 TLS 证书的使用者名称或使用者替代名称相匹配。

如果值不匹配，将其替换成正确的值。

4 重新启动 VMware Horizon View PCoIP 安全网关服务，使所做更改生效。

后续步骤

将 CA 签发的证书导入到 Windows 本地计算机证书存储区，并配置证书友好名称。

在 Windows 证书存储区中配置 PSG 证书

要将默认的 PSG 证书替换为 CA 签发的证书，必须在运行 PSG 的连接服务器或安全服务器计算机上的 Windows 本地计算机证书存储区中配置证书及其私钥。

如果您希望 PSG 使用唯一的证书，则必须使用可导出私钥将证书导入到 Windows 本地计算机证书存储区内，并设置相应的友好名称。

如果您希望 PSG 使用与服务器相同的证书，则不必遵循此步骤。但是，您必须在 Windows 注册表中将服务器名设置为与服务器证书使用者名称相匹配，并将友好名称设置为 **vdm**。

前提条件

- 确认证书长度不少于 1024 位。
- 确认 TLS 证书有效。服务器计算机上的当前时间必须在证书的开始和结束日期范围内。
- 确认证书使用者名称或其中一个使用者替代名称与 Windows 注册表中的 `SSLCertPsgSni` 设置相匹配。请参阅确认服务器名称与 PSG 证书使用者名称相匹配。
- 确认证书插件已添加至 MMC。请参阅将证书管理单元添加到 MMC。
- 熟悉将证书导入到 Windows 证书存储区的步骤。请参阅将签名的服务器证书导入到 Windows 证书存储区。
- 熟悉修改证书友好名称的步骤。请参阅修改证书的友好名称。

步骤

1. 在 Windows Server 主机上的 MMC 窗口中，打开**证书 (本地计算机) > 个人**文件夹。
2. 选择**更多操作 > 所有任务 > 导入**，以导入颁发给 PSG 的 TLS 证书。

   在**证书导入**向导中选择下列设置：

   a **将此密钥标记为可导出**

   b **包含所有可扩展属性**

   结束向导，完成将证书导入**个人**文件夹
3. 通过以下步骤之一确认新证书含有私钥：
   - 确认证书图标上显示有黄色钥匙图案。
   - 双击证书，确认在“证书信息”对话框中显示有以下声明：您有一个与该证书对应的私钥。
4. 右键单击新证书，然后单击**属性**。
5. 在“常规”选项卡下，删除**友好名称**文本，并输入您选择的友好名称。

   确保您所输入的名称与 Windows 注册表中的 `SSLCertWinCertFriendlyName` 设置完全相同，具体步骤见下方。
6. 单击**应用**，然后单击**确定**。

PSG 会将 CA 签发的证书提供给通过 PCoIP 连接至服务器的客户端设备。

注　这一步骤不影响旧版客户端设备。PSG 会继续将默认的旧版证书提供给通过 PCoIP 连接至此服务器的旧版客户端设备。

后续步骤

在 Windows 注册表中配置证书友好名称。

在 Windows 注册表中设置 PSG 证书友好名称

PSG 会通过服务器名称和证书友好名称识别要使用的 TLS 证书。您必须在运行 PSG 的连接服务器或安全服务器计算机上的 Windows 注册表中设置友好名称值。

所有连接服务器实例和安全服务器均使用 **vdm** 这一证书友好名称。您可通过比较为 PSG 证书配置自己的证书友好名称。您必须对 Windows 注册表设置进行配置才能让 PSG 将正确的名称与您即将在 Windows 证书存储区中设置的友好名称相匹配。

PSG 可使用与运行 PSG 的服务器所使用的相同 TLS 证书。如果您将 PSG 配置为使用与该服务器相同的证书，则友好名称必须是 **vdm**。

注册表和 Windows 证书存储区中的友好名称值均区分大小写。

前提条件

- 确认 Windows 注册表中包含用于访问 PSG 端口的正确使用者名称，且该名称与 PSG 证书使用者名称或使用者替代名称相匹配。请参阅确认服务器名称与 PSG 证书使用者名称相匹配。
- 确认已在 Windows 本地计算机证书存储区内配置证书友好名称。请参阅在 Windows 证书存储区中配置 PSG 证书。

步骤

1. 在运行 PCoIP 安全网关的连接服务器或安全服务器计算机上启动 Windows 注册表编辑器。
2. 导航至 `HKEY_LOCAL_MACHINE\SOFTWARE\Teradici\SecurityGateway` 注册表项。
3. 为此注册表项添加新字符串 (REG_SZ) 值：`SSLCertWinCertFriendlyName`。
4. 修改 `SSLCertWinCertFriendlyName` 值，并输入要由 PSG 使用的证书友好名称。

   例如：**pcoip**

   如果使用与该服务器相同的证书，则该值必须是 **vdm**。
5. 重新启动 VMware Horizon View PCoIP 安全网关服务，使所做更改生效。

后续步骤

确认客户端设备可继续连接 PSG。

如果您要使用安全扫描程序进行合规性测试，请扫描 PSG 端口。

（可选）与 PSG 连接时强制使用 CA 签发的证书

您可以确保与 PSG 的所有客户端连接均对 PSG 使用 CA 签发的证书，而不是默认的旧版证书。此步骤不是为 PSG 配置 CA 签发证书的必需步骤。只有需要在您的 Horizon 7 部署中强制使用 CA 签发的证书时，才采取这些步骤。

在某些情况下，PSG 可能会向安全服务器提供默认的旧版证书，而不是 CA 签发的证书，从而造成 PSG 端口的合规性测试失效。要解决这一问题，您可配置 PSG 使其不向尝试与其进行连接的设备提供默认旧版证书。

重要 执行此步骤可阻止所有旧版客户端通过 PCoIP 连接本服务器。

前提条件

确认包括瘦客户端在内的所有连接到此服务器的客户端设备均运行适用于 Windows 的 Horizon Client 5.2 或 Horizon Client 2.0 或更高版本。您必须对旧版客户端进行升级。

步骤

1 在运行 PCoIP 安全网关的连接服务器或安全服务器计算机上启动 Windows 注册表编辑器。

2 导航至 `HKEY_LOCAL_MACHINE\SOFTWARE\Teradici\SecurityGateway` 注册表项。

3 为此注册表项添加新字符串 (REG_SZ) 值：`SSLCertPresentLegacyCertificate`。

4 将 `SSLCertPresentLegacyCertificate` 的值设置为 **0**。

5 重新启动 VMware Horizon View PCoIP 安全网关服务，使所做更改生效。

将 Horizon Administrator 设置为信任 vCenter Server 或 View Composer 证书

在 Horizon Administrator 控制板中，可以将 Horizon 7 配置为信任不受信任的 vCenter Server 或 View Composer 证书。

VMware 强烈建议将 vCenter Server 和 View Composer 配置为使用 CA 签发的 TLS 证书。或者，您也可以接受 vCenter Server 或 View Composer 的默认证书的指纹。

同样，VMware 建议将 SAML 2.0 身份验证器配置为使用 CA 签发的 TLS 证书。或者，您也可以在 Horizon Administrator 控制板中通过接受默认证书的指纹，将 Horizon 7 配置为信任不受信任的 SAML 2.0 服务器证书。

使用 CA 签发的 TLS 证书的优势

CA 是确保证书及其创建者身份的受信机构。如果证书是由受信任的 CA 签发，则系统不会向用户显示要求验证证书的消息，且瘦客户端设备可以在无需额外配置的情况下进行连接。

您可以请求特定于某个 Web 域（如 `www.mycorp.com`）的 TLS 服务器证书，或者也可以请求可在整个域（如 `*.mycorp.com`）中使用的通配符 TLS 服务器证书。为简化管理，如果需要在多台服务器上或不同子域中安装证书，您可以选择请求通配符证书。

通常情况下，在安全安装中使用特定于域的证书，与通配符证书相比，CA 通常可以更好地保护特定于域的证书，使其免于丢失。如果使用与其他服务共享的通配符证书，则 Horizon 7 产品的安全性还取决于其他服务的安全性。如果使用通配符证书，必须确保私钥可以在服务器之间传输。

将默认证书替换为您的个人证书后，客户端会使用该证书对服务器进行身份验证。如果您的证书是由 CA 签发，那么 CA 本身的证书通常会嵌入在浏览器中，或是位于客户端可以访问的可信数据库中。客户端接受证书后，会通过发送密钥（由证书中的公钥加密）来做出响应。此密钥用于加密客户端和服务器之间的流量。

Horizon 连接服务器和安全服务器上的证书问题故障排除

Horizon 7 Server 上的证书问题会妨碍您连接到 Horizon Administrator，或者导致服务器运行状况指示器显示为红色。

问题

您无法连接到有问题的连接服务器实例上的 Horizon Administrator。连接到同一个容器中其他连接服务器实例上的 Horizon Administrator 时，可以看到有问题的连接服务器实例的控制板运行状况指示器显示为红色。

从其他连接服务器实例中，单击红色的运行状况指示器会显示 SSL 证书：无效 (SSL Certificate: Invalid) 和状态：(Status:)（空白），以指示找不到有效的证书。Horizon 7 日志文件中包含一个类型为“错误”且具有以下错误文本的日志条目：密钥存储中没有合格的证书 (No qualifying certificates in keystore)。

Horizon 7 日志数据位于连接服务器实例上的 C:\ProgramData\VMware\VDM\logs\log-*.txt 中。

原因

由于以下任意原因，证书可能未成功安装到 Horizon 7 服务器上：

- 证书不在 Windows 本地计算机证书存储区的 Personal 文件夹中。
- 证书存储区中没有证书的私钥。
- 证书没有友好名称 **vdm**。
- 证书是从 Windows Server 2008 或更高版本服务器的 v3 证书模板生成。Horizon 7 无法检测私钥，但如果您使用证书插件检查 Windows 证书存储区，该存储区会指示有私钥。

解决方案

- 确认该证书导入到 Windows 本地计算机证书存储区的 Personal 文件夹中。

  请参阅将签名的服务器证书导入到 Windows 证书存储区。
- 确认证书包含私钥。

  请参阅将签名的服务器证书导入到 Windows 证书存储区。
- 确认证书具有友好名称 **vdm**。

  请参阅修改证书的友好名称。
- 如果证书是从 v3 证书模板生成，则从 CA 获取不使用 v3 模板的有效签名证书。

  请参阅获取 CA 签发的 TLS 证书。

为订阅许可证启用 Horizon 7

9

您可以部署 Horizon 7 订阅许可证以用于 Horizon 7 内部部署或 VMware Cloud on AWS 上的部署。

Horizon 7 订阅许可证可为同一产品提供更高的部署灵活性。通过 Horizon 7 订阅许可证，可在数据中心、私有云和 VMware Horizon Cloud Service 上部署 Horizon 7。

本章讨论了以下主题：

- VMware Horizon 7 Cloud Connector
- 使用 Horizon 7 部署 Horizon 7 Cloud Connector 虚拟设备
- 为 Horizon 7 Cloud Connector root 用户设置密码到期策略
- 为 Horizon 7 Cloud Connector 虚拟设备配置 CA 签名的证书

VMware Horizon 7 Cloud Connector

Horizon 7 Cloud Connector 是一个可将 Horizon 7 容器与 VMware Horizon Cloud Service 连接起来的虚拟设备。Horizon 7 Cloud Connector 是桥接 Horizon 7 容器和 VMware Horizon Cloud Service 的必备组件。云托管服务（包括 Horizon 7 订阅许可证、运行状况仪表板和 Horizon Help Desk Tool）需要使用 Horizon 7 Cloud Connector。

您必须拥有有效的 My VMware 帐户才能从 https://my.vmware.com 购买 Horizon 7 许可证。购买后，您会收到一封订阅电子邮件，其中包含可以作为 OVA 文件下载 Horizon 7 Cloud Connector 的链接。

从 vSphere Web Client 部署 Horizon 7 Cloud Connector 虚拟设备时，需要将 Cloud Connector 与希望连接到 Horizon Cloud Service 的连接服务器容器进行配对。在配对过程中，Horizon 7 Cloud Connector 虚拟设备会将连接服务器连接到 Horizon Cloud Service 以管理 Horizon 7 订阅许可证和其他服务。使用 Horizon 7 订阅许可证，您无需手动输入用于 VMware Horizon 7 产品激活的 Horizon 7 许可证密钥。但是，您需要使用这些许可证密钥来激活支持组件，例如，vSphere 和 App Volumes 等。

注　Horizon 7 Cloud Connector 虚拟设备不支持 IPv6 环境。

使用 Horizon 7 部署 Horizon 7 Cloud Connector 虚拟设备

购买订阅许可证后，您将收到一封许可证订阅电子邮件，其中包含可下载 Horizon 7 Cloud Connector 虚拟设备的链接。您可以安装 Horizon 7 Cloud Connector 虚拟设备，并将其与容器中的连接服务器进行配对。

前提条件

- Horizon 7 版本 7.6 或更高版本。
- 您必须在 https://my.vmware.com 上有一个 My VMware 帐户才能购买 Horizon 7 订阅许可证。
- 从 my.vmware.com 发送给您的订阅许可证电子邮件中下载 Horizon 7 Cloud Connector 虚拟设备。
- 验证要将 Horizon 7 Cloud Connector 虚拟设备与之配对的连接服务器。您一次只能将 Horizon 7 Cloud Connector 虚拟设备与内部部署容器中安装的一个连接服务器进行配对。
- 如果 Horizon 7 Cloud Connector 虚拟设备不属于连接服务器所加入的 Active Directory 域，请将要与 Horizon 7 Cloud Connector 配对的连接服务器的 FQDN 添加到 Horizon 7 Cloud Connector 虚拟设备上的 `/etc/hosts` 文件。
- 如果您使用 Microsoft Internet Explorer Web 浏览器，请确认兼容性模式已关闭，这样才能查看 Horizon 7 Cloud Connector 设备用户界面。
- 部署具有静态 IP 的 Horizon 7 Cloud Connector 虚拟设备，并将该设备加入 Active Directory。在开始部署之前，请在 Active Directory 的 DNS 中添加 Horizon 7 Cloud Connector 虚拟设备的正向和反向查找条目。

步骤

1. 从您帐户的订阅电子邮件中提供的链接下载 Horizon 7 Cloud Connector 设备。可作为 OVA 文件下载 Horizon 7 Cloud Connector 设备。
2. 使用 vSphere Web Client 将 Horizon 7 Cloud Connector 设备部署为 OVF 模板。有关部署 OVF 模板的更多信息，请参阅《vSphere 虚拟机管理》文档。

   注　输入 OVF 模板的 root 密码时，必须确认密码至少包含八个字符，其中包括一个大写字母、一个数字和一个特殊字符。

3. 在 vSphere Web Client 中，打开 Horizon 7 Cloud Connector 设备的电源。

   将显示 Horizon 7 Cloud Connector 设备用户界面 IP 地址。
4. 在 Web 浏览器中，输入 Horizon 7 Cloud Connector 设备的 IP 地址以登录到 Horizon 7 Cloud Connector 用户界面。

   使用您的 My VMware 帐户凭据登录。
5. 将 Horizon 7 Cloud Connector 设备与内部部署的连接服务器实例相连接。在**连接到 Horizon 7 连接服务器**框中，输入内部部署托管的连接服务器的 FQDN，然后单击**连接**。
6. 单击此复选框以验证连接服务器的指纹证书。

   注　如果连接服务器具有有效的根 CA 证书，将跳过此验证步骤。

7. 输入连接服务器的域名、用户名和密码，然后单击**连接**。

   注　为了更好地审核 Horizon 7 Cloud Connector 操作，请使用连接服务器的唯一用户名和密码。

8 （可选）如果连接服务器已与另一 Horizon 7 Cloud Connector 设备配对，请单击**接受**以删除现有配对，然后将其与您下载的 Horizon 7 Cloud Connector 设备配对。

9 要在 Horizon Cloud Service 上设置 Horizon 7 容器，请输入节点的名称，选择数据中心位置，然后输入可选描述。

Horizon 7 容器已成功与 VMware Horizon Cloud Service 配对。

10 （可选）要在同一个容器中重新配置连接服务器详细信息，请单击**重新配置**，并按照步骤操作以完成向导。

注 为了防止无法应用订阅许可证，如果替换连接服务器的自签名证书，您还必须为该容器重新配置连接服务器详细信息。如果将自签名证书替换为自定义 CA 签名证书，则不需要执行该步骤。要配置自定义 CA 签名证书，请参阅为 Horizon 7 Cloud Connector 虚拟设备配置 CA 签名的证书。

11 （可选）要移除内部部署连接服务器与 Horizon Cloud Service 之间的连接，请单击**拔出**。

注 请不要在单击**拔出**之前从 vCenter Server 删除 Horizon 7 Cloud Connector 虚拟设备。

后续步骤

- 在 Horizon Administrator 中查看订阅许可证详细信息。有关更多信息，请参阅《Horizon 7 管理指南》文档。
- 如果您需要升级到最新版本的 Horizon 7 Cloud Connector 虚拟设备，请参阅《Horizon 7 升级指南》文档。
- 要登录到 Horizon Cloud 管理控制台，请参阅《VMware Horizon Cloud Service on Microsoft Azure 管理指南》（网址为 https://docs.vmware.com/cn/VMware-Horizon-Cloud-Service/index.html ）。

为 Horizon 7 Cloud Connector root 用户设置密码到期策略

您可以在部署期间为 Horizon 7 Cloud Connector 虚拟设备的 root 用户设置密码。默认情况下，该密码不会过期。不过，根据用户的安全策略，您可能需要为 root 用户设置到期策略以定期更新 root 密码。

注 在登录到 Horizon 7 Cloud Connector 虚拟设备后，您必须以 root 用户身份输入所有命令。如果用户设置自定义密码到期策略，在密码到期之前，由您负责以管理员身份定期登录并更新密码。
Horizon 7 Cloud Connector 虚拟设备不会向管理员通知密码到期。

步骤

1 要为 root 用户设置密码到期策略，请输入以下命令：

```
chage –M <Max days before password change> –W <Number of days of warning before password expires>
root
```

例如，如果您希望密码在密码更改日期之后的 365 天到期，并且在密码到期之前设置 30 天的警告期，请输入以下命令：

```
chage –M 365 –W 30 root
```

2 要列出 root 用户的当前密码到期策略，请输入以下命令：

```
chage -l root
```

为 Horizon 7 Cloud Connector 虚拟设备配置 CA 签名的证书

为了增强安全性，您可以为 Horizon 7 Cloud Connector 虚拟设备配置自定义的 CA 签名证书。

前提条件

- 确认有 PEM 格式的完整证书链可用。
- 确认有 PEM 格式的私钥可用。
- 确认所颁发的证书中包含 FQDN 和主体备用名称。

步骤

1 打开一个与 Horizon 7 Cloud Connector 虚拟设备的 SSH 会话。

2 复制目录 `/root/server.crt` 中的 CA 签名证书。

3 复制目录 `/root/server.key` 中的 CA 签名密钥。

4 备份现有证书。

使用以下命令：

```
cp /etc/nginx/ssl/server.crt /etc/nginx/ssl/server.crt.orig
```

5 备份现有密钥。

使用以下命令：

```
cp /etc/nginx/ssl/server.key /etc/nginx/ssl/server.key.orig
```

6 复制现有 `nginx conf` 文件。

使用以下命令：

```
cp /etc/nginx/nginx.conf /etc/nginx/nginx.conf.orig
```

7 复制 `/etc/nginx/ssl` 目录中的 CA 证书。

使用以下命令：

```
cp /root/server.crt /etc/nginx/ssl/server.crt
```

8 复制 `/etc/nginx/ssl` 目录中的 CA 证书密钥文件。

使用以下命令：

```
cp /root/server.key /etc/nginx/ssl/server.key
```

9 确认证书和密钥文件的所有者和权限。

使用以下命令：

```
chown –R root:root /etc/nginx/ssl
```

```
chmod –R 600 /etc/nginx/ssl
```

10 确认证书中颁发的 FQDN 与位于 `/etc/nginx/nginx.conf` 的 `nginx` 配置文件内的服务器侦听 443 块中的服务器名称指令相匹配。

11 检查并重新启动 `nginx`。

使用以下命令：

```
nginx –t
```

```
systemctl restart nginx
```

12 通过在 Web 浏览器中重新加载 Horizon 7 Cloud Connector 用户界面 URL，对新证书进行测试。

13 （可选）如果证书可正常使用，请移除备份的文件。

使用以下命令：

```
rm /etc/nginx/ssl/server.crt.orig
```

```
rm /etc/nginx/ssl/server.key.orig
```

```
rm /etc/nginx/nginx.conf.orig
```

14 移除根目录中复制的 CA 证书和密钥文件。

使用以下命令：

```
rm /root/server.crt
```

```
rm /root/server.key
```

首次配置 Horizon 7

10

为服务器安装 Horizon 7 Server 软件并配置 SSL 证书后，必须采取一些额外的步骤来设置有效的 Horizon 7 环境。

您可以为 vCenter Server 和 View Composer 配置用户帐户、安装 Horizon 7 许可证密钥、将 vCenter Server 和 View Composer 添加至您的 Horizon 7 环境、配置 PCoIP 安全网关和安全加密链路，以及对 Windows Server 进行大小设置以支持您的 Horizon 7 环境（可选）。

本章讨论了以下主题：

- 为 vCenter Server、View Composer 和即时克隆配置用户帐户
- 首次配置 Horizon 连接服务器
- 配置 Horizon Client 连接
- 替换 Horizon 7 服务的默认端口
- 调整 Windows Server 设置以支持您的部署

为 vCenter Server、View Composer 和即时克隆配置用户帐户

要配合使用 vCenter Server 和 Horizon 7，您必须配置拥有合适的 vCenter Server 特权的用户帐户。可以创建拥有合适特权的 vCenter Server 角色，并将该角色分配给 vCenter Server 用户帐户。

如果 View Composer 与 vCenter Server 安装在不同计算机上，您还必须在 Active Directory 中创建一个用户帐户，Horizon 7 可使用该用户帐户对独立计算机上的 View Composer 服务进行身份验证。

如果使用 View Composer，则必须在 Active Directory 中创建第三个用户帐户，以允许 View Composer 在 Active Directory 中执行特定操作。View Composer 需要使用该帐户将链接克隆虚拟机加入到您的 Active Directory 域中。请参阅为 View Composer AD 操作创建用户帐户。

如果您使用即时克隆，则必须在 Active Directory 中创建一个用户帐户，以允许连接服务器在 Active Directory 中执行特定操作。连接服务器需要使用该帐户将即时克隆虚拟机加入到您的 Active Directory 域中。请参阅为即时克隆操作创建用户帐户。

总而言之，首次配置 Horizon 7 时，您需要在 Horizon Administrator 中提供以下用户帐户：

- vCenter Server 用户允许 Horizon 7 和 View Composer 在 vCenter Server 中执行操作。

- 独立的 View Composer Server 用户允许 Horizon 7 对独立计算机上的 View Composer 服务进行身份验证。

  如果 View Composer 与 vCenter Server 安装在同一计算机上，则 vCenter Server 用户可执行上述两个功能，并且无需使用独立的 View Composer Server 用户。
- AD 操作的 View Composer 用户允许 View Composer 在 Active Directory 中执行特定操作。
- AD 操作的即时克隆用户允许连接服务器在 Active Directory 中执行特定操作。

使用 vCenter Server 用户和 View Composer 用户的位置

创建并配置这些用户帐户后，需要在 Horizon Administrator 中指定用户名。

- 将 vCenter Server 添加到 Horizon 7 时，需要指定一个 vCenter Server 用户。
- 配置 View Composer 设置并选择**独立的 View Composer Server** 时，指定一个独立的 View Composer Server 用户。
- 配置 View Composer 域时，为 AD 操作指定 View Composer 用户。
- 创建链接克隆池时，为 AD 操作指定 View Composer 用户。

为 Horizon 7 和 View Composer 配置 vCenter Server 用户

要配置一个使 Horizon 7 有权在 vCenter Server 中执行操作的用户帐户，您必须为该用户分配一个拥有合适特权的 vCenter Server 角色。

必须添加到 vCenter Server 角色的特权列表各不相同，具体取决于您是否通过 View Composer 使用 Horizon 7。View Composer 服务要在 vCenter Server 中执行操作，必须具备除基本特权之外的特权。

如果 View Composer 与 vCenter Server 安装在同一计算机上，则必须将 vCenter Server 用户作为 vCenter Server 计算机上的本地系统管理员。此要求允许 Horizon 7 对 View Composer 服务进行身份验证。

如果 View Composer 与 vCenter Server 安装在不同计算机上，则无需将 vCenter Server 用户作为 vCenter Server 计算机上的本地管理员。但是，您必须创建独立的 View Composer Server 用户帐户，且该用户帐户必须是 View Composer 计算机上的本地管理员。

前提条件

- 在 Active Directory 中，在连接服务器域或受信任的域中创建一个用户。请参阅为 vCenter Server 创建用户帐户。
- 熟悉此用户帐户所需的 vCenter Server 特权。请参阅 vCenter Server 用户所需的特权。
- 如果使用 View Composer，请熟悉所需的其他特权。请参阅 vCenter Server 用户所需的 View Composer 和即时克隆特权。

步骤

1 在 vCenter Server 中，为用户准备一个拥有所需特权的角色。

- 您可以使用 vCenter Server 中预定义的 Administrator 角色。该角色可以执行 vCenter Server 中所有的操作。
- 如果您使用 View Composer，您可以创建一个权利有限的角色，为其授予连接服务器和 View Composer 执行 vCenter Server 操作所需的最低特权。

  在 vSphere Client 中，单击**主页 > 角色 > 添加角色**，输入角色名称（如 **`View Composer Administrator`**），然后为此角色选择特权。

  此角色必须拥有连接服务器和 View Composer 在 vCenter Server 中运行所需的所有特权。
- 如果您使用不带 View Composer 的 Horizon 7，您可以创建一个权利更小的角色，为其授予连接服务器执行 vCenter Server 操作所需的最低特权。

  在 vSphere Client 中，单击**主页 > 角色 > 添加角色**，输入角色名称（如 **`View Manager Administrator`**），然后为该此角色选择特权。
- 如果您使用即时克隆，可以创建一个权利有限的角色，为其授予连接服务器执行 vCenter Server 操作所需的最低特权。

  在 vSphere Client 中，单击**主页 > 角色 > 添加角色**，输入角色名称（如 **`View Manager 即时克隆管理员`**），然后为该角色选择特权。有关即时克隆的特权，请参阅 vCenter Server 用户所需的 View Composer 和即时克隆特权。

2 在 vSphere Client 中，右键单击清单顶层的 vCenter Server，单击**添加权限**，然后添加 vCenter Server 用户。

> **注** 您必须在 vCenter Server 级别定义 vCenter Server 用户。

3 在下拉菜单中选择您创建的管理员角色、View Composer 或 View Manager 角色，并将其分配给 vCenter Server 用户。

4 如果 View Composer 与 vCenter Server 安装在同一计算机上，请添加 vCenter Server 用户帐户作为 vCenter Server 计算机上本地系统管理员组的成员。

  如果 View Composer 与 vCenter Server 安装在不同计算机上，则无需此执行步骤。

后续步骤

在 Horizon Administrator 中将 vCenter Server 添加到 Horizon 7 时，指定 vCenter Server 用户。请参阅将 vCenter Server 实例添加到 Horizon 7。

vCenter Server 用户所需的特权

vCenter Server 用户必须具有足够的 vCenter Server 特权，才能使 Horizon 7 可以在 vCenter Server 中执行操作。为 vCenter Server 用户创建一个拥有所需特权的 View Manager 角色。

表 10-1. View Manager 角色所需的特权

特权组	您需要启用的特权
文件夹	创建文件夹 删除文件夹
数据存储	分配空间
虚拟机	在**配置**中： ■ **添加或移除设备** ■ **高级** ■ **修改设备设置** 在**交互**中： ■ **关闭电源** ■ **打开电源** ■ **重置** ■ **挂起** ■ **执行擦除或压缩操作** 在**清单**中： ■ **新建** ■ **从现有创建** ■ **移除** 在**置备**中： ■ **自定义** ■ **部署模板** ■ **读取自定义规范** ■ **克隆模板** ■ **克隆虚拟机**
资源	**将虚拟机分配给资源池**
全局	**充当 vCenter Server** 即使您不使用 View Storage Accelerator，vCenter Server 用户也需要具备此特权。
主机	实施启用了 ESXi 主机缓存的 View Storage Accelerator 时，需要使用以下**主机**特权。如果不使用 View Storage Accelerator，vCenter Server 用户将不需要此特权。 在**配置**中： ■ **高级设置**
配置文件驱动存储（如果使用的是 vSAN 数据存储或虚拟卷）	（全部）

vCenter Server 用户所需的 View Composer 和即时克隆特权

要支持 View Composer 或即时克隆，vCenter Server 用户还必须拥有支持 Horizon 7 所需的特权之外的相应特权。

“View Composer 和即时克隆特权”列出了 View Manager、View Composer 和即时克隆所需的特权超集。

表 10-2. View Composer 和即时克隆特权

vCenter Server 上的特权组	您需要启用的特权
文件夹	**创建文件夹** **删除文件夹**
数据存储 表 10-2	**分配空间** **浏览数据存储** **低级别文件操作**
主机	在**清单**中 ■ **修改群集**
虚拟机	在**配置**中（全部） 在**交互**中： ■ **关闭电源** ■ **打开电源** ■ **重置** ■ **挂起** ■ **执行擦除或压缩操作** ■ **设备连接** 在**清单**中（全部） 在**快照管理**中（全部） 在**置备**中： ■ **自定义** ■ **部署模板** ■ **读取自定义规范** ■ **克隆模板** ■ **克隆虚拟机** ■ **允许访问磁盘**
资源	**将虚拟机分配给资源池** 执行 View Composer 重新平衡操作需要下列特权。 **迁移已关闭电源的虚拟机**
全局	**启用方法** **禁用方法** **系统标记** **管理自定义属性** **设置自定义属性** 实施启用 ESXi 主机缓存的 View Storage Accelerator 时，需要使用以下特权。即使您不使用 View Storage Accelerator，vCenter Server 用户也需要具备此特权。 **充当 vCenter Server**
网络	（全部）
配置文件驱动存储	（全部 - 如果使用的是 vSAN 数据存储或虚拟卷）

表 10-2. View Composer 和即时克隆特权 （续）

vCenter Server 上的特权组	您需要启用的特权
存储视图	查看
加密操作	如果您使用包含可信的平台模块 (vTPM) 设备的即时克隆虚拟机，则需要具备以下特权。 ■ 克隆 ■ 解密 ■ 直接访问 ■ 加密 ■ 管理 KMS ■ 迁移

首次配置 Horizon 连接服务器

安装连接服务器后，必须安装产品许可证，并将 vCenter Server 和 View Composer 服务添加到 Horizon 7。还可以允许 ESXi 主机回收链接克隆虚拟机上的磁盘空间，并配置 ESXi 主机，使其对虚拟机磁盘数据进行缓存。

如果安装安全服务器，它们将自动添加到 Horizon 7 并显示在 Horizon Administrator 中。

Horizon Administrator 和 Horizon 连接服务器

Horizon Administrator 为 Horizon 7 提供了基于 Web 的管理界面。

Horizon 连接服务器可以具有多个实例来作为副本服务器或安全服务器。根据您的 Horizon 7 部署，您可以对每个连接服务器实例获取一个 Horizon Administrator 界面。

可使用以下最佳做法将 Horizon Administrator 与连接服务器配合使用：

- 使用连接服务器的主机名和 IP 地址登录到 Horizon Administrator。使用 Horizon Administrator 界面管理连接服务器以及任何关联的安全服务器或副本服务器。
- 在容器环境中，确认所有管理员使用同一连接服务器的主机名和 IP 地址登录到 Horizon Administrator。不要使用负载平衡器的主机名和 IP 地址访问 Horizon Administrator 网页。
- 为了确定您所使用的连接服务器容器，您可以查看 Horizon Administrator 标题和 Web 浏览器选项卡中的容器名称。

注 如果使用 Unified Access Gateway 设备而不是安全服务器，您必须使用 Unified Access Gateway REST API 管理 Unified Access Gateway 设备。早期版本的 Unified Access Gateway 称为 Access Point。有关更多信息，请参阅《部署和配置 Unified Access Gateway》。

登录到 Horizon Administrator

要执行初始配置任务，必须登录到 Horizon Administrator。

前提条件

确认您使用的是 Horizon Administrator 支持的 Web 浏览器。请参阅 Horizon Administrator 要求。

步骤

1 打开 Web 浏览器并输入以下 URL，其中 *server* 是连接服务器实例的主机名。

`https://server/admin`

注 当主机名不可解析时，如果您需要访问连接服务器实例，则可以使用 IP 地址。但是，您连接的主机将与为连接服务器实例配置的 TLS 证书不匹配，从而导致访问被阻止或访问的安全性降低。

对 Horizon Administrator 的访问取决于连接服务器计算机上配置的证书类型。

如果在连接服务器主机上打开 Web 浏览器，请使用 **`https://127.0.0.1`**（而非 **`https://localhost`**）进行连接。该方法可以避免在解析 `localhost` 时遭受潜在 DNS 攻击，从而提高安全性。

选项	说明
为 View 连接服务器配置一个由 CA 签发的证书。	首次连接时，您的 Web 浏览器会显示 Horizon Administrator。
配置了 View 连接服务器提供的默认自签名证书。	第一次连接时，Web 浏览器可能会显示一个页面，警告与该地址相关联的安全证书不是由受信任的证书颁发机构颁发的。 单击**忽略**可继续使用当前的 TLS 证书。

2 使用具有管理员角色的帐户登录。

当您在副本组中安装独立的连接服务器实例或第一个连接服务器实例时，可以为管理员角色指定首个分配。默认情况下，会选择安装连接服务器时使用的帐户，但您也可以将此帐户更改为管理员本地组或域的全局组。

如果您选择管理员本地组，那么您可以使用直接添加到此组或通过全局组成员资格添加到此组的任何域用户。您不能使用添加到此组的本地用户。

登录到 Horizon Administrator 后，您可以使用 **View 配置 > 管理员**来更改具有管理员角色的用户和组列表。

安装产品许可证密钥

您必须先输入产品许可证密钥，然后才能使用连接服务器。

注 如果您拥有 Horizon 7 订阅许可证，则不需要产品许可证密钥。有关订阅许可证的更多信息，请参阅第 9 章，为订阅许可证启用 Horizon 7。

首次登录时，Horizon Administrator 会显示“产品许可和使用情况”页面。

安装许可证密钥后，Horizon Administrator 将在您登录时显示控制板页面。

安装连接服务器副本实例或安全服务器时，不需要配置许可证密钥。副本实例和安全服务器使用存储在 View LDAP 配置中的通用许可证密钥。

注 连接服务器需要有效的许可证密钥。产品许可证密钥是一个包含 25 个字符的密钥。

步骤

1 在 Horizon Administrator 中，选择 **View 配置 > 产品许可和使用情况**。

2 在**许可**面板中，单击**编辑许可证**。

3 输入许可证序列号，然后单击**确定**。

4 验证许可证的过期日期。

5 根据产品许可证授权您使用的 VMware Horizon 7 版本，验证是启用还是禁用了桌面、应用程序远程处理和 View Composer 许可证。

并非所有版本都提供 VMware Horizon 7 的所有特性和功能。有关各个版本中的功能集的比较，请参阅 http://www.vmware.com/files/pdf/products/horizon-view/VMware-Horizon-View-Pricing-Licensing-FAQ.pdf。

将 vCenter Server 实例添加到 Horizon 7

您必须将 Horizon 7 配置为连接到 Horizon 7 部署中的 vCenter Server 实例。vCenter Server 可创建并管理 Horizon 7 在桌面池中使用的虚拟机。

如果是在链接模式组中运行 vCenter Server 实例，就必须将每个 Horizon 7 实例分别添加到 View Manager。

Horizon 7 使用安全通道 (SSL) 连接至 vCenter Server 实例。

前提条件

- 安装连接服务器产品许可证密钥。
- 准备一个有权在 vCenter Server 中执行支持 Horizon 7 所需操作的 vCenter Server 用户。要使用 View Composer，您必须为该用户授予额外的特权。

  请参阅为 Horizon 7 和 View Composer 配置 vCenter Server 用户。
- 确认 vCenter Server 主机上安装了 TLS/SSL 服务器证书。在生产环境中，安装由受信任证书颁发机构 (Certificate Authority, CA) 签名的有效证书。

  在测试环境中，您可以使用随 vCenter Server 一起安装的默认证书，但在 Horizon 7 中添加 vCenter Server 时必须接受证书指纹。
- 确认副本组中的所有连接服务器实例都信任 vCenter Server 主机上安装的服务器证书的根 CA 证书。检查根 CA 证书是否位于连接服务器主机上 Windows 本地计算机证书存储区中的**受信任的根证书颁发机构 > 证书**文件夹中。如果没有，请将根 CA 证书导入 Windows 本机证书存储区。

  请参阅将根证书和中间证书导入 Windows 证书存储区。
- 确认 vCenter Server 实例包含 ESXi 主机。如果 vCenter Server 实例中未配置主机，则无法在 Horizon 7 中添加实例。
- 如果您要升级到 vSphere 5.5 或更高版本，请确认您用作 vCenter Server 用户的域管理员帐户已由 vCenter Server 本地用户明确分配了登录 vCenter Server 的权限。
- 如果您计划以 FIPS 模式使用 Horizon 7，请确认您具有 vCenter Server 6.0 或更高版本以及 ESXi 6.0 或更高版本的主机。

  有关更多信息，请参阅第 4 章，以 FIPS 模式安装 Horizon 7。

- 熟悉用于确定 vCenter Server 和 View Composer 最大操作数限制的设置。请参阅 vCenter Server 和 View Composer 的并发操作数限制和设置并发电源操作率来支持远程桌面登录风暴。

步骤

1 在 Horizon Administrator 中，选择 **View 配置 > 服务器**。

2 在 **vCenter Server** 选项卡上，单击**添加**。

3 在 vCenter Server 设置**服务器地址**文本框中，键入 vCenter Server 实例的完全限定域名 (FQDN)。

FQDN 包含主机名和域名。例如，在 FQDN ***myserverhost.companydomain.com*** 中，***myserverhost*** 是主机名，***companydomain.com*** 是域名。

注 如果通过 DNS 名称或 URL 来输入服务器，则 Horizon 7 不会执行 DNS 查找来确认管理员之前是否是使用 IP 地址将该服务器添加到 Horizon 7 中的。如果同时使用 DNS 名称和 IP 地址添加 vCenter Server，则会发生冲突。

4 键入 vCenter Server 用户的名称。

例如：**domain\user** 或 **user@domain.com**

5 键入 vCenter Server 用户密码。

6 （可选）键入该 vCenter Server 实例的描述。

7 键入 TCP 端口号。

默认端口为 443。

8 在“高级设置”下，设置 vCenter Server 和 View Composer 操作的并发操作数限制。

9 单击**下一步**显示 View Composer 设置页面。

后续步骤

配置 View Composer 设置。

- 如果为 vCenter Server 实例配置了 SSL 签名证书，且连接服务器信任根证书，则“添加 vCenter Server”向导会显示“View Composer 设置”页面。
- 如果为 vCenter Server 实例配置了默认证书，则必须先确定是否接受现有证书的指纹。请参阅接受默认 TLS 证书的指纹。

如果 Horizon 7 使用多个 vCenter Server 实例，请重复执行此步骤添加其他 vCenter Server 实例。

配置 View Composer 设置

要使用 View Composer，必须配置允许连接服务器连接到 View Composer 服务的设置。View Composer 可安装在独立的计算机上，也可与 vCenter Server 安装在同一计算机上。

VMware 建议在每个 View Composer 服务和 vCenter Server 实例之间建立一对一的映射关系。

前提条件

- 确认已将连接服务器配置为连接到 vCenter Server。为此，您必须完成“添加 vCenter Server”向导中的“vCenter Server 信息”页面。请参阅将 vCenter Server 实例添加到 Horizon 7。
- 确认该 View Composer 服务尚未配置为连接到不同的 vCenter Server 实例。
- 如果在独立的计算机上安装 View Composer，请确认已创建独立的 View Composer Server 用户帐户。此域用户帐户必须是 View Composer 计算机上本地管理员组的成员。

步骤

1 在 Horizon Administrator 中，完成“添加 vCenter Server”向导中的“vCenter Server 信息”页面。

   a 单击 **View 配置 > 服务器**。

   b 在“vCenter Server”选项卡中，单击**添加**并提供 vCenter Server 设置。

2 在“View Composer 设置”页面上，如果您未使用 View Composer，则请选择**不使用 View Composer**。

   如果选择**不使用 View Composer**，则其他的 View Composer 设置将无效。单击**下一步**后，“添加 vCenter Server”向导会显示“存储设置”页面，但不会显示“View Composer 域”页面。

3 如果使用 View Composer，请选择 View Composer 计算机的位置。

选项	说明
View Composer 与 vCenter Server 安装在同一计算机上。	a 选择 **View Composer 与 vCenter Server 一同安装**。 b 确保端口号与您在 vCenter Server 上安装 View Composer 服务时指定的端口号相一致。默认端口号为 18443。
View Composer 安装在独立的计算机上。	a 选择**独立的 View Composer Server**。 b 在 View Composer Server 地址文本框中，键入 View Composer 计算机的完全限定域名 (FQDN)。 c 键入可以对 View Composer 服务进行身份验证的域用户帐户的名称。 此帐户必须是独立 View Composer 计算机上本地管理员组的成员。 例如：**`domain.com\user`** 或 **`user@domain.com`** d 键入此域用户帐户的密码。 e 确保端口号与您安装 View Composer 服务时指定的端口号相一致。默认端口号为 18443。

4 单击**下一步**显示“View Composer 域”页面。

后续步骤

配置 View Composer 域。

- 如果为 View Composer 实例配置了 SSL 签名证书，且连接服务器信任根证书，则“添加 vCenter Server”向导会显示“View Composer 域”页面。
- 如果为 View Composer 实例配置了默认证书，则必须先确定是否接受现有证书的指纹。请参阅接受默认 TLS 证书的指纹。

配置 View Composer 域

您必须配置一个 Active Directory 域，以便 View Composer 在其中部署链接克隆桌面。可以为 View Composer 配置多个域。先将 vCenter Server 和 View Composer 设置添加到 View 后，即可通过在 Horizon Administrator 中编辑 vCenter Server 实例来添加更多 View Composer 域。

前提条件

- 您的 Active Directory 管理员必须为 AD 操作创建 View Composer 用户。此域用户必须具有在包含链接克隆的 Active Directory 域中添加和移除虚拟机的权限。有关此用户所需权限的信息，请参阅为 View Composer AD 操作创建用户帐户。
- 在 Horizon Administrator 中，确认您已完成“添加 vCenter Server”向导中的“vCenter Server 信息”和“View Composer 设置”页面。

步骤

1 在“View Composer 域”页面中，单击**添加**为 AD 操作帐户信息添加 View Composer 用户。

2 键入 Active Directry 域的域名。

例如：**domain.com**

3 键入 View Composer 用户的域用户名，包括域名。

例如：**domain.com\admin**

4 键入帐户密码。

5 单击**确定**。

6 要添加在部署链接克隆池的其他 Active Directory 域中具有特权的域用户帐户，请重复以上的步骤。

7 单击**下一步**显示“存储设置”页面。

后续步骤

启用虚拟机磁盘空间回收，并为 Horizon 7 配置 View Storage Accelerator。

添加即时克隆域管理员

必须先向 Horizon 7 中添加即时克隆域管理员，然后才能创建即时克隆桌面池。

即时克隆域管理员必须具有一定的 Active Directory 域特权。

步骤

1 在 Horizon Administrator 中，选择 **View 配置 > 即时克隆域管理员**。

2 单击**添加**。

3 输入即时克隆域管理员的登录名和密码。

允许 vSphere 回收链接克隆虚拟机中的磁盘空间

在 vSphere 5.1 及更高版本中，可以启用 Horizon 7 的磁盘空间回收功能。从 vSphere 5.1 开始，Horizon 7 能够以高效的磁盘格式创建链接克隆虚拟机，这种磁盘格式允许 ESXi 主机回收链接克隆中未使用的磁盘空间，从而减少链接克隆所需的总存储空间。

随着用户与链接克隆桌面的交互，克隆的操作系统磁盘会逐渐增大，最终会使用几乎与完整克隆桌面相同的磁盘空间。磁盘空间回收有助于减少操作系统磁盘的大小，无需刷新或重构链接克隆。在虚拟机处于开启状态时以及用户与远程桌面交互时，都可以回收空间。

对于无法利用存储空间节省策略（例如，注销时刷新）的部署来说，磁盘空间回收功能尤其有用。例如，在专用远程桌面上安装用户应用程序的知识型员工在远程桌面刷新或重构时，可能会丢失自己的个人应用程序。通过磁盘空间回收，Horizon 7 可以将链接克隆的大小保持在接近于这些克隆初次置备后启动时的较小大小。

此功能由两部分组成：节省空间的磁盘格式和空间回收操作。

在 vSphere 5.1 或更高版本环境中，如果父虚拟机的虚拟硬件版本为 9 或更高版本，无论是否启用空间回收操作，Horizon 7 都会创建具有能节省空间的操作系统磁盘的链接克隆。

要启用空间回收操作，您必须使用 Horizon Administrator 启用 vCenter Server 的空间回收，并回收各桌面池的虚拟机磁盘空间。vCenter Server 的空间回收设置支持您在所有受 vCenter Server 实例管理的桌面池上禁用此功能。禁用 vCenter Server 的该功能会覆盖桌面池级别的设置。

以下指导原则适用于空间回收功能：

- 仅对链接克隆上能节省空间的操作系统磁盘有效。
- 这不会影响 View Composer 永久磁盘。
- 仅适用于 vSphere 5.1 或更高版本且虚拟硬件版本为 9 或更高版本的虚拟机。
- 不适用于完整克隆桌面。
- 适用于具有 SCSI 控制器的虚拟机。不支持 IDE 控制器。

如果池中包含具有能节省空间的磁盘的虚拟机，则不支持 View Composer Array Integration (VCAI)。VCAI 使用 vStorage APIs for Array Integration (VAAI) 本地 NFS 快照技术克隆虚拟机。

前提条件

- 确认 vCenter Server 和 ESXi 主机（包括群集中的所有 ESXi 主机）版本为 5.1，且具有 ESXi 5.1 下载补丁程序 ESXi510-201212001 或更高版本。

步骤

1 在 Horizon Administrator 中，完成“添加 vCenter Server”向导中“存储设置”页面之前的各页面。

   a 选择 **View 配置 > 服务器**。

   b 在 **vCenter Server** 选项卡上，单击**添加**。

   c 完成“vCenter Server 信息”、“View Composer 设置”和“View Composer 域”三个页面。

2 在“存储设置”页面中，确保选中**启用空间回收**。

如果是全新安装 Horizon 7 5.2 或更高版本，默认已选中空间回收功能。如果是从 Horizon 7 5.1 或更早版本升级到 Horizon 7 5.2 或更高版本，则必须选中**启用空间回收**。

后续步骤

在?存储设置?页面中配置 View Storage Accelerator。

要完成 Horizon 7 中的磁盘空间回收配置，需要为桌面池设置空间回收。

为 vCenter Server 配置 View Storage Accelerator

在 vSphere 5.1 及更高版本中，可以将 ESXi 主机配置为缓存虚拟机磁盘数据。这项称为 View Storage Accelerator 的功能可以使用 ESXi 主机中的 Content Based Read Cache (CBRC) 功能。View Storage Accelerator 可以在发生 I/O 风暴（大量虚拟机同时启动或同时运行多个防病毒扫描时可能会发生）时提高 Horizon 7 性能。对于需要频繁加载应用程序或数据的管理员或用户来说，这项功能同样有益。主机不再从存储系统中一遍遍地读取整个操作系统或应用程序，而是从缓存中读取常规数据块。

通过在引导风暴时减少 IOPS 数量，View Storage Accelerator 降低了对存储阵列的需求，使您可以用更少的存储 I/O 带宽支持 Horizon 7 部署。

按照此过程中所述，在 Horizon Administrator 中选择 vCenter Server 向导中的 View Storage Accelerator 设置，启用 ESXi 主机上的缓存功能。

确保也为单独的桌面池配置了 View Storage Accelerator。要对某个桌面池进行操作，必须针对 vCenter Server 和该桌面池启用 View Storage Accelerator。

默认情况下，已为桌面池启用 View Storage Accelerator。可以在创建或编辑池时禁用或启用此功能。最佳方法是在首次创建桌面池时启用此功能。如果通过编辑现有池来启用此功能，您必须确保先创建新副本及其摘要磁盘，再置备链接克隆。可以通过将池重构为新的快照或者将池重新平衡为新的数据存储来创建新副本。仅当桌面池中的虚拟机处于关闭状态时，才能为它们配置摘要文件。

您可以在包含链接克隆的桌面池和包含完整虚拟机的桌面池中启用 View Storage Accelerator。

启用了 View Storage Accelerator 的池不支持本地 NFS 快照技术 (VAAI)。

View Storage Accelerator 现在可在使用 Horizon 7 副本分层的配置下运行，在此配置中，副本存储于单独的数据存储中，而不是链接克隆中。虽然将 Horizon 7 副本分层与 View Storage Accelerator 搭配使用在性能方面并没有太大的实质性提升，但是通过将副本存储到单独的数据存储，还是能够带来一些容量方面的好处。因此，我们对这种组合方式进行了测试，并提供支持。

重要 如果您计划使用此功能，并且正在使用多个共享某些 ESXi 主机的 Horizon 7 容器，则必须为共享的 ESXi 主机上的所有池启用 Horizon Storage Accelerator 功能。如果多个容器中的设置不一致，可能会导致共享 ESXi 主机上的虚拟机出现不稳定。

前提条件

- 确认 vCenter Server 和 ESXi 主机版本为 5.1 或更高。

  在 ESXi 群集中，确认所有主机的版本均为 5.1 或更高。

- 确认在 vCenter Server 中为 vCenter Server 用户分配了**主机 > 配置 > 高级设置**特权。

  请参阅为 vCenter Server、View Composer 和即时克隆配置用户帐户。

步骤

1 在 Horizon Administrator 中，完成“添加 vCenter Server”向导中“存储设置”页面之前的各页面。

   a 选择 **View 配置 > 服务器**。

   b 在 **vCenter Server** 选项卡上，单击**添加**。

   c 完成“vCenter Server 信息”、“View Composer 设置”和“View Composer 域”三个页面。

2 在“存储设置”页面上，确保选中**启用 View Storage Accelerator** 复选框。

   该复选框默认为选中。

3 指定默认的主机缓存大小。

   默认的缓存大小适用于此 vCenter Server 实例管理的所有 ESXi 主机。

   默认值为 1,024 MB。缓存大小必须在 100 MB 和 2,048 MB 之间。

4 要为单个 ESXi 主机指定不同的缓存大小，请选择 ESXi 主机并单击**编辑缓存大小**。

   a 在“主机缓存”对话框中，选中 **覆盖默认主机缓存大小**。

   b 键入一个介于 100 MB 和 2,048 MB 之间的**主机缓存大小**值，并单击**确定**。

5 在“存储设置”页面上，单击**下一步**。

6 单击**完成**在 Horizon 7 中添加 vCenter Server、View Composer 和存储设置。

后续步骤

要配置客户端连接的 PCoIP 安全网关、安全加密链路和外部 URL，请参阅配置 Horizon Client 连接。

要完成 Horizon 7 中的 View Storage Accelerator 设置，请为桌面池配置 View Storage Accelerator。请参阅《在 Horizon 7 中设置虚拟桌面》文档中的“为桌面池配置 View Storage Accelerator”。

vCenter Server 和 View Composer 的并发操作数限制

在将 vCenter Server 添加到 Horizon 7 或编辑 vCenter Server 设置时，您可以配置多个选项，这些选项用来设置由 vCenter Server 和 View Composer 所执行的并发操作的最大数量。

您可以在 vCenter Server 信息页上的“高级设置”面板中配置这些选项。

表 10-3. vCenter Server 和 View Composer 的并发操作数限制

设置	说明
最大并发 vCenter 置备操作数量	确定连接服务器在此 vCenter Server 实例中置备和删除完整虚拟机时可以发出的最大并发请求数。 默认值为 20。 此设置仅适用于完整的虚拟机。
最大并发电源操作数量	确定此 vCenter Server 实例中的连接服务器所管理的虚拟机上可以发生的最大并发电源操作数（启动、关闭、挂起等）。 默认值为 50。 有关计算该设置的值的指导原则，请参阅设置并发电源操作率来支持远程桌面登录风暴。 此设置适用于完整的虚拟机和链接克隆。
最大并发 View Composer 维护操作数量	确定在此 View Composer 实例所管理的链接克隆上可以发生的最大并发 View Composer 刷新、重构和重新平衡操作数。 默认值为 12。 必须先注销包含活动会话的远程桌面，然后才能开始维护操作。如果强制用户在维护操作开始时立即注销，则需要注销的远程桌面上的最大并发操作数将只达到所配置的值的一半。例如，如果将此设置配置为 24，并强制用户注销，则需要注销的远程桌面上的最大并发操作数为 12。 此设置仅适用于链接克隆。
最大并发 View Composer 置备操作数量	确定在此 View Composer 实例所管理的链接克隆上可以发生的最大并发创建和删除操作数。 默认值为 8。 此设置仅适用于链接克隆。

设置并发电源操作率来支持远程桌面登录风暴

最大并发电源操作数量设置用于控制可在 vCenter Server 实例的远程桌面虚拟机上发生的最大并发电源操作数量。这一限制默认设置为 50。当大量用户同时登录其桌面时，可更改此值以支持开机峰值速率。

作为最佳实践，您可通过试运行来确定此设置的正确值。有关规划指导原则，请参阅《Horizon 7 架构规划指南》文档中的“体系结构设计元素与规划指导原则”。

所需并发电源操作数量基于桌面开启的峰值速率，以及桌面开启、引导到可供连接所花费的时间。总之，建议的电源操作限制值就是桌面启动所花费的总时间乘以开机峰值速率。

例如，桌面的平均启动时间在二到三分钟之间。因此，并发电源操作限制值应是开机峰值速率的 3 倍。默认设置 50 应该可支持每分钟 16 个桌面的开机峰值速率。

系统等待桌面启动的最长时间为五分钟。如果启动时间更长的话，有可能会出现其他错误。为了保守起见，您可将并发电源操作限制值设为开机峰值速率的 5 倍。采用这种谨慎方法，默认设置 50 可以支持每分钟 10 个桌面的开机峰值速率。

登录操作以及桌面开启操作，通常会平均分布在特定时段内。您可以估算开机峰值速率，方法是：假设开机峰值发生在时段中间，在此期间大约 40% 的开机操作发生在该时段的 1/6 时间内。例如，如果用户在上午 8:00 到 9:00 之间登录，时段为一小时，40% 的登录操作会发生在上午 8:25 到 8:35 这 10 分钟之内。如果有 2000 名用户，其中 20% 的用户关闭了桌面，那么这 400 个桌面开启操作中会有 40% 发生在这 10 分钟之内。开机峰值速率为每分钟 16 个桌面。

接受默认 TLS 证书的指纹

在向 Horizon 7 添加 vCenter Server 和 View Composer 实例时，必须确保用于 vCenter Server 和 View Composer 实例的 TLS 证书有效且受连接服务器信任。如果随 vCenter Server 和 View Composer 一起安装的默认证书仍然存在，则必须确定是否接受这些证书的指纹。

如果为 vCenter Server 或 View Composer 实例配置了 CA 签发的证书，且根证书受连接服务器信任，则无需接受证书指纹。无需采取任何操作。

如果使用 CA 签发的证书替换默认证书，但连接服务器不信任根证书，则必须确定是否接受证书指纹。指纹是证书的加密哈希值。通过指纹可以快速确定提供的证书是否与另一个证书（例如之前接受的证书）相同。

注　如果您在同一 Windows Server 主机上安装 vCenter Server 和 View Composer，它们可以使用相同的 TLS 证书，但必须单独为每个组件配置证书。

有关配置 TLS 证书的详细信息，请参阅 第 8 章，为 Horizon 7 Server 配置 TLS 证书。

您首先需要使用“添加 vCenter Server”向导在 Horizon Administrator 中添加 vCenter Server 和 View Composer。如果证书不受信任而您也未接受指纹，则无法添加 vCenter Server 和 View Composer。

添加这些服务器后，您可以在“编辑 vCenter Server”对话框中重新配置它们。

注　从较早的版本进行升级时，如果 vCenter Server 或 View Composer 证书不受信任，或者您使用不受信任的证书替换了受信任证书，您也必须接受证书指纹。

在 Horizon Administrator 控制板上，vCenter Server 或 View Composer 图标会变为红色，并会显示“检测到无效的证书”对话框。在 Horizon Administrator 中，单击 **View 配置 > 服务器**，并编辑与 View Composer 服务关联的 vCenter Server 条目。然后，单击 vCenter Server 设置中的**编辑**，按照提示确认并接受自签名的证书。

同样，在 Horizon Administrator 中，您可以配置 SAML 身份验证器供连接服务器实例使用。如果 SAML 服务器证书不受连接服务器信任，您必须确定是否接受证书指纹。如果不接受指纹，就无法在 Horizon 7 中配置 SAML 身份验证器。配置 SAML 身份验证器后，您可以在“编辑连接服务器”对话框中重新配置它。

步骤

1. 当 Horizon Administrator 显示“检测到无效的证书”对话框时，单击**查看证书**。
2. 检查“证书信息”窗口中的证书指纹。
3. 检查为 vCenter Server 或 View Composer 实例配置的证书指纹。
   a. 在 vCenter Server 或 View Composer 主机上，启动 MMC 插件并打开 Windows 证书存储区。
   b. 导航至 vCenter Server 或 View Composer 证书。
   c. 单击“证书详细信息”选项卡显示证书指纹。

   同样还需要检查 SAML 身份验证器的证书指纹。如果可以，请针对 SAML 身份验证器主机执行之前的步骤。

4 验证“证书信息”窗口中的指纹是否与 vCenter Server 或 View Composer 实例的指纹相匹配。

同样还需要验证这些指纹是否与 SAML 身份验证器相匹配。

5 确定是否接受证书指纹。

选项	说明
指纹匹配。	单击**接受**以使用默认证书。
指纹不匹配。	单击**拒绝**。 对不匹配的证书进行故障排除。例如，您可能为 vCenter Server 或 View Composer 提供了错误的 IP 地址。

配置 Horizon Client 连接

客户端端点通过安全连接与连接服务器或安全服务器主机通信。

用于用户身份验证以及远程桌面和应用程序选择的初始客户端连接将在用户向 Horizon Client 提供域名时通过 HTTPS 创建。如果您网络环境中的防火墙和负载平衡软件配置正确，此请求将会发送到连接服务器或安全服务器主机。通过该连接可实现用户身份验证以及桌面或应用程序选取，但不会将用户连接到远程桌面或应用程序。

用户连接到远程桌面和应用程序时，客户端会默认建立另一个到连接服务器或安全服务器主机的连接。此连接提供了一条通过 HTTPS 传送 RDP 数据和其他数据的安全加密链路，因此称作安全加密链路连接。

用户通过 PCoIP 显示协议连接到远程桌面和应用程序时，客户端可进一步连接到连接服务器或安全服务器主机上的 PCoIP 安全网关。PCoIP 安全网关可确保只有经过身份验证的用户才能通过 PCoIP 与远程桌面和应用程序进行通信。

您还可以向通过 VMware Blast 显示协议连接到远程桌面和应用程序的用户，以及使用 HTML Access 连接到远程桌面的外部用户提供安全连接。Blast 安全网关可确保只有经过身份验证的用户才能与远程桌面进行通信。

根据使用的客户端设备的类型，建立更多通道以传送其他流量，如传送 USB 重定向数据至客户端设备。如果启用安全加密链路，则这些数据通道将通过它传送流量。

禁用安全加密链路和安全网关后，桌面和应用程序会话将绕过连接服务器或安全服务器主机，而直接在客户端设备和远程计算机之间建立。这种连接类型被称为直接连接。

即使连接服务器不再运行，直接连接的桌面和应用程序会话也会保持连接。

通常情况下，为了通过 WAN 向连接到安全服务器或连接服务器主机的外部客户端提供安全连接，您需要启用安全加密链路、PCoIP 安全网关和 Blast 安全网关。您可以禁用安全加密链路和安全网关来允许连接 LAN 的内部客户端与远程桌面和应用程序建立直接连接。

如果仅启用安全加密链路或仅启用一个安全网关，则会话可能会根据使用的客户端类型，对某些流量使用直接连接，而通过连接服务器或安全服务器主机发送其他流量。

所有客户端在连接到连接服务器和安全服务器主机时都需要使用 SSL。

配置 PCoIP 安全网关和安全加密链路连接

您可以使用 Horizon Administrator 配置是否使用安全加密链路和 PCoIP 安全网关。这些组件可确保只有经过身份验证的用户才能与远程桌面和应用程序进行通信。

使用 PCoIP 显示协议的客户端可以使用 PCoIP 安全网关。使用 RDP 显示协议的客户端可以使用安全加密链路。

有关配置 Blast 安全网关的更多信息，请参阅配置 Blast 安全网关。

重要 为外部客户端提供安全连接的常规网络配置通常都包含安全服务器。要启用或禁用安全服务器上的安全加密链路和 PCoIP 安全网关，必须编辑与安全服务器配对的连接服务器实例。

在外部客户端直接连接到连接服务器主机的网络配置中，可以通过在 Horizon Administrator 中编辑该连接服务器实例来启用或禁用安全加密链路和 PCoIP 安全网关。

前提条件

- 如果您打算启用 PCoIP 安全网关，请确认连接服务器实例以及与其配对的安全服务器为 View 4.6 或更高版本。
- 如果您要将某个安全服务器与一个已启用 PCoIP 安全网关的连接服务器实例进行配对，请确认该安全服务器为 View 4.6 或更高版本。

步骤

1 在 Horizon Administrator 中，选择 **View 配置 > 服务器**。

2 在“连接服务器”面板中，选择连接服务器实例，然后单击**编辑**。

3 配置是否使用安全加密链路连接。

选项	说明
禁用安全加密链路连接	取消选中**使用安全加密链路连接计算机**。
启用安全加密链路连接	选择**使用安全加密链路连接计算机**。

默认情况下，安全加密链路连接为启用状态。

4 配置是否使用 PCoIP 安全网关。

选项	说明
启用 PCoIP 安全网关	选中**使用 PCoIP 安全网关与计算机建立 PCoIP 连接**。
禁用 PCoIP 安全网关	取消选中**使用 PCoIP 安全网关与计算机建立 PCoIP 连接**。

默认禁用 PCoIP 安全网关。

5 单击**确定**保存更改。

配置 Blast 安全网关

在 Horizon Administrator 中，您可以配置使用 Blast 安全网关来提供对远程桌面和应用程序的安全访问（通过 HTML Access，或通过使用 VMware Blast 显示协议的客户端连接）。

Blast 安全网关包含 Blast Extreme 自适应传输 (BEAT) 网络连接，可进行动态调整以适应网络条件，例如不断变化的网速和数据包丢失。

- 仅当在 Unified Access Gateway 设备上运行时，Blast 安全网关才支持 BEAT 网络连接。
- 连接到 Unified Access Gateway 设备版本 3.3 或更高版本时，可以同时在 TCP 端口 8443 上和 UDP 端口 8443（对于 BEAT）上处理使用 IPv4 的 Horizon Client 和使用 IPv6 的 Horizon Client。
- 使用典型网络条件的 Horizon Client 必须连接到连接服务器（BSG 被禁用）、安全服务器（BSG 被禁用）或版本高于 2.8 的 Unified Access Gateway 设备。如果 Horizon Client 使用典型的网络条件连接到连接服务器（BSG 已启用）、安全服务器（BSG 已启用）或版本低于 2.8 的 Unified Access Gateway 设备，该客户端会自动检测网络条件，并回退至 TCP 网络连接。
- 使用较差网络条件的 Horizon Client 必须连接到版本为 2.9 或更高版本的 Unified Access Gateway 设备（已启用 UDP Tunnel Server）。如果 Horizon Client 使用较差的网络条件连接到连接服务器（BSG 已启用）、安全服务器（BSG 已启用）或版本低于 2.8 的 Unified Access Gateway 设备，该客户端会自动检测网络条件，并回退至 TCP 网络连接。
- Horizon Client 使用较差的网络条件连接到连接服务器（BSG 被禁用）、安全服务器（BSG 被禁用）或版本为 2.9 或更高版本的 Unified Access Gateway 设备（已启用 UDP Tunnel Server），或版本为 2.8 的 Unified Access Gateway 设备，该客户端会自动检测网络条件，并回退至典型的网络条件。

有关详细信息，请参阅 https://docs.vmware.com/cn/VMware-Horizon-Client/index.html 网址上的 Horizon Client 文档。

注 您还可以使用 Unified Access Gateway 设备而不是安全服务器，对 Horizon 7 服务器和桌面进行安全外部访问。如果使用 Unified Access Gateway 设备，您必须在连接服务器实例上禁用安全网关，并在 Unified Access Gateway 设备上启用这些网关。有关更多信息，请参阅《部署和配置 Unified Access Gateway》。

如果未启用 Blast 安全网关，客户端设备和客户端 Web 浏览器会使用 VMware Blast Extreme 协议绕过 Blast 安全网关，而与远程桌面虚拟机和应用程序建立直接连接。

重要 为外部用户提供安全连接的常规网络配置通常都包含安全服务器。要启用或禁用安全服务器上的 Blast 安全网关，您必须编辑与安全服务器配对的连接服务器实例。如果外部用户直接连接到连接服务器主机，可以通过编辑该连接服务器实例来启用或禁用 Blast 安全网关。

前提条件

如果用户使用 VMware Identity Manager 选择了远程桌面，请确认 VMware Identity Manager 已安装并配置与连接服务器配合使用，且连接服务器已与 SAML 2.0 身份验证服务器配对。

步骤

1 在 Horizon Administrator 中，选择 **View 配置 > 服务器**。

2 在**连接服务器**选项卡上，选择连接服务器实例，并单击**编辑**。

3 配置是否使用 Blast 安全网关。

选项	说明
启用 Blast 安全网关	选择**使用 Blast 安全网关对计算机进行 Blast 连接**
为 HTML Access 启用 Blast 安全网关	选择**使用 Blast 安全网关仅对计算机进行 HTML Access Blast 连接**
禁用 Blast 安全网关	选择**不使用 Blast 安全网关**

默认情况下，Blast 安全网关为启用状态。

4 单击**确定**保存更改。

为安全网关和安全加密链路连接配置外部 URL

要使用安全加密链路，客户端系统必须能够访问 IP 地址或可解析为 IP 地址的完全限定域名 (FQDN)，以便客户端连接到连接服务器或安全服务器主机。

要使用 PCoIP 安全网关，客户端需要使用 URL 连接到连接服务器或安全服务器主机。在 IPv4 环境中，URL 必须按主机的 IP 地址来标识主机。在 IPv6 环境中，URL 可以按主机的 IP 地址或 FQDN 来标识主机。

要使用 Blast 安全网关，用户的端点设备必须能够访问可解析为 IP 地址的 FQDN，该地址可使用户的 Web 浏览器或计算机连接到连接服务器或安全服务器主机。

从外部使用安全加密链路连接

默认情况下，仅位于同一网络、因而能够查找请求的主机的安全加密链路客户端可以连接到连接服务器或安全服务器主机。

很多机构都希望用户能通过特定的 IP 地址、客户端可以解析的域名及特定的端口来实现外部连接。该信息可能类似于连接服务器或安全服务器主机的实际地址和端口号，也可能并不与它们类似。可通过 URL 的形式提供给客户端系统。例如：

- `https://view-example.com:443`
- `https://view.example.com:443`
- `https://example.com:1234`
- `https://10.20.30.40:443`

要在 Horizon 7 中使用此类地址，您必须将连接服务器或安全服务器主机配置为返回外部 URL 而不是主机 FQDN。

配置外部 URL

可以配置多个外部 URL。第一个 URL 允许客户端系统建立安全加密链路连接。第二个 URL 允许使用 PCoIP 的客户端通过 PCoIP 安全网关建立安全连接。在 IPv4 环境中，URL 必须按主机的 IP 地址来标识主机。在 IPv6 环境中，URL 可以按主机的 IP 地址或 FQDN 来标识主机。URL 允许客户端从外部位置进行连接。

第三个 URL 允许用户通过 Blast 安全网关从自己的客户端设备或 Web 浏览器建立安全连接。

如果您的网络配置中包含安全服务器，请为安全服务器提供外部 URL。与安全服务器配对的连接服务器实例无需使用外部 URL。

连接服务器实例和安全服务器的外部 URL 配置过程有所不同。

- 对于连接服务器实例，您可以通过在 Horizon Administrator 中编辑连接服务器设置来设置外部 URL。
- 对于安全服务器，您可以在运行连接服务器安装程序时设置外部 URL。您可以使用 Horizon Administrator 修改安全服务器的外部 URL。

设置连接服务器实例的外部 URL

您可以使用 Horizon Administrator 配置连接服务器实例的外部 URL。

安全加密链路外部 URL、PCoIP 外部 URL 和 Blast 外部 URL 都必须是客户端系统用于访问此连接服务器实例的地址。

前提条件

- 确认在连接服务器实例上启用了安全加密链路连接和 PCoIP 安全网关。请参阅配置 PCoIP 安全网关和安全加密链路连接。
- 要设置 Blast 外部 URL，请确认在连接服务器实例上启用了 Blast 安全网关。请参阅配置 Blast 安全网关。

步骤

1 在 Horizon Administrator 中，单击 **View 配置 > 服务器**。

2 在“连接服务器”选项卡中，选择连接服务器实例，然后单击**编辑**。

3 在**外部 URL** 文本框中键入安全加密链路的外部 URL。

URL 必须包含协议、客户端可解析的主机名和端口号。

例如：`https://myserver.example.com:443`

注 当主机名不可解析时，如果您需要访问连接服务器实例，则可以使用 IP 地址。但是，您连接的主机将与为连接服务器实例配置的 TLS 证书不匹配，从而导致访问被阻止或访问的安全性降低。

4 在 **PCoIP 外部 URL** 文本框中键入 PCoIP 安全网关的外部 URL。

在 IPv4 环境中，指定 PCoIP 外部 URL 作为 IP 地址，端口号为 4172。在 IPv6 环境中，可以指定 IP 地址或完全限定域名，端口号为 4172。在两种环境中，都不要包含协议名称。

例如，在 IPv4 环境中：`10.20.30.40:4172`

客户端必须能够使用 URL 访问安全服务器。

5 在 **Blast 外部 URL** 文本框中键入 Blast 安全网关的外部 URL。

URL 必须包含 HTTPS 协议、客户端可解析的主机名和端口号。

例如：`https://myserver.example.com:8443`

默认情况下，URL 包含安全加密链路外部 URL 的 FQDN 和默认端口号 8443。URL 中必须包含客户端系统可用于访问此连接服务器主机的 FQDN 和端口号。

6 确认此对话框中的所有地址都允许客户端系统访问此连接服务器实例。

7 单击**确定**。

修改安全服务器的外部 URL

您可以使用 Horizon Administrator 修改安全服务器的外部 URL。

这些外部 URL 最初是在连接服务器安装程序中安装安全服务器时配置的。

安全加密链路外部 URL、PCoIP 外部 URL 和 Blast 外部 URL 都必须是客户端系统用于连接此安全服务器的地址。

前提条件

- 确认与此安全服务器配对的连接服务器实例上已启用安全加密链路连接和 PCoIP 安全网关。请参阅配置 PCoIP 安全网关和安全加密链路连接。
- 要设置 Blast 外部 URL，请确认与此安全服务器配对的连接服务器实例上已启用 Blast 安全网关。请参阅配置 Blast 安全网关。

步骤

1 在 Horizon Administrator 中，选择 **View 配置 > 服务器**。

2 在“安全服务器”选项卡中，选择安全服务器并单击**编辑**。

3 在**外部 URL** 文本框中键入安全加密链路的外部 URL。

URL 必须包含协议、客户端可解析的安全服务器主机名和端口号。

例如：`https://myserver.example.com:443`

注 如果您需要在主机名不可解析时访问安全服务器，可以使用 IP 地址。但您连接的主机将与为安全服务器实例配置的 TLS 证书不匹配，导致访问被阻止或访问的安全性降低。

4 在 **PCoIP 外部 URL** 文本框中键入 PCoIP 安全网关的外部 URL。

在 IPv4 环境中，指定 PCoIP 外部 URL 作为 IP 地址，端口号为 4172。在 IPv6 环境中，可以指定 IP 地址或域名，端口号为 4172。在两种环境中，都不要包含协议名称。

例如，在 IPv4 环境中：`10.20.30.40:4172`

客户端必须能够使用 URL 访问安全服务器。

5 在 **Blast 外部 URL** 文本框中键入 Blast 安全网关的外部 URL。

URL 必须包含 HTTPS 协议、客户端可解析的主机名和端口号。

例如：`https://myserver.example.com:8443`

默认情况下，URL 包含安全加密链路外部 URL 的 FQDN 和默认端口号 8443。URL 必须包含客户端系统可用来连接此安全服务器的 FQDN 和端口号。

6 确认此对话框中的所有地址都允许客户端系统连接此安全服务器主机。

7 单击**确定**保存更改。

Horizon Administrator 会将更新的外部 URL 发送到安全服务器。您无需重新启动安全服务器，所做的更改即可生效。

Horizon 连接服务器返回地址信息时优先返回 DNS 名称

默认情况下，将桌面计算机和 RDS 主机的地址发送到客户端和网关时，Horizon 连接服务器会优先返回 IP 地址。您可以使用 Horizon 7 LDAP 属性更改此默认行为，要求 Horizon 连接服务器优先返回 DNS 名称。在某些环境中，要求连接服务器将 DNS 名称返回到客户端和网关能够为网络基础架构设计带来更多灵活性。

注　此 Horizon 7 LDAP 属性替代了 Horizon 6.0.*x* 和更早版本中由组策略设置 `Connect using DNS Name` 提供的按桌面功能。

Horizon 7 LDAP 属性会影响在连接服务器实例（而不是安全服务器）上运行适用于 Windows 的 Horizon Client 3.3 或更高版本、HTML Access 3.5 或更高版本及安全网关的客户端。

前提条件

请参阅 Microsoft TechNet 网站，了解如何在您的 Windows Server 操作系统版本上使用“ADSI 编辑”实用程序。

步骤

1. 在您的连接服务器计算机上启动“ADSI 编辑”实用程序。
2. 在控制台树中，选择**连接到**。
3. 在**选择或键入可分辨名称或命名上下文**文本框中，键入可分辨名称 **DC=vdi, DC=vmware, DC=int**。
4. 在**选择或键入域或服务器**文本框中，选择或键入 **`localhost:389`** 或连接服务器计算机的完全限定域名 (FQDN)，后跟端口 389。

   例如：`localhost:389` 或 `mycomputer.mydomain.com:389`
5. 在对象 **CN=Common, OU=Global, OU=Properties** 上，将 **pae-PreferDNS** 属性值设为 1。

   将此属性设为 1 后，如果存在 DNS 名称且接收方支持名称解析，连接服务器将返回 DNS 名称。否则，如果存在适用于您环境（IPv4 或 IPv6）的类型正确的 IP 地址，连接服务器将返回 IP 地址。

   当此属性未设置或设为 0 时，如果存在类型正确的 IP 地址，连接服务器将返回 IP 地址。否则，将返回 IP 地址兼容性错误。

允许 HTML Access 通过负载平衡器

在用户使用 HTML Access 时，直接位于负载平衡器或负载平衡的网关后面的连接服务器实例和安全服务器必须知道浏览器连接到负载平衡器时使用的地址。

对于直接位于网关后面的连接服务器实例和安全服务器，请执行允许 HTML Access 通过网关中所述的步骤。

您必须为位于负载平衡器或负载平衡的网关后面的每个 Horizon 7 Server 执行该步骤。

步骤

1 在连接服务器或安全服务器主机的 SSL 网关配置文件夹中创建或编辑 `locked.properties` 文件。

例如，*`install_directory`*`\VMware\VMware View\Server\sslgateway\conf\locked.properties`。

2 添加 `balancedHost` 属性并将其设置为负载平衡器地址。

例如，如果用户在浏览器中键入 **`https://view.example.com`** 以访问任何负载平衡的 Horizon 7 Server，请将 `balancedHost=view.example.com` 添加到 `locked.properties` 文件中。

3 保存 `locked.properties` 文件。

4 重新启动 Horizon 连接服务器服务或安全服务器服务，使所做的更改生效。

允许 HTML Access 通过网关

在用户使用 HTML Access 时，直接位于网关（如 Access Point）后面的连接服务器实例和安全服务器必须知道浏览器连接到网关时使用的地址。

对于位于负载平衡器或负载平衡的网关后面的连接服务器实例和安全服务器，请执行允许 HTML Access 通过负载平衡器中所述的步骤。

您必须为位于网关后面的每个 Horizon 7 Server 执行该步骤。

步骤

1 在连接服务器或安全服务器主机的 SSL 网关配置文件夹中创建或编辑 `locked.properties` 文件。

例如，*`install_directory`*`\VMware\VMware View\Server\sslgateway\conf\locked.properties`。

2 添加 `portalHost` 属性并将其设置为网关地址。

例如，如果 `https://view-gateway.example.com` 是浏览器通过网关访问 Horizon 7 时使用的地址，请将 `portalHost=view-gateway.example.com` 添加到 `locked.properties` 文件中。

如果连接服务器实例或安全服务器位于多个网关后面，您可以在 `portalHost` 属性中添加一个数字以指定每个网关，例如：

```
portalHost.1=view-gateway-1.example.com
portalHost.2=view-gateway-2.example.com
```

如果已知单个网关计算机具有多个名称，您还必须指定多个 `portalHost` 属性。

3 保存 `locked.properties` 文件。

4 重新启动 Horizon 连接服务器服务或安全服务器服务，使所做的更改生效。

替换 Horizon 7 服务的默认端口

安装过程中，View 服务的默认设置是在特定网络端口进行侦听。在某些组织中，必须更改这些端口以遵循组织策略或避免争用问题。您可以更改连接服务器、安全服务器、PCoIP 安全网关和 View Composer 服务使用的默认端口。

更改端口是一项可选的设置任务。如果部署未要求更改，则使用默认端口。

有关 Horizon 7 Server 使用的默认 TCP 和 UDP 端口列表，请参阅《Horizon 7 安全指南》文档。

替换 Horizon 连接服务器实例和安全服务器的默认 HTTP 端口或网卡

可以通过编辑服务器计算机上的 `locked.properties` 文件来替换连接服务器实例或安全服务器的默认 HTTP 端口或网卡。贵组织可能要求您执行这些任务以遵循组织策略或避免争用问题。

默认 SSL 端口为 443。默认非 SSL 端口为 80。

本步骤中所做的端口更改不会影响安全加密链路外部 URL 中指定的端口。根据您的网络配置，可能还需要更改安全加密链路外部 URL 端口。

如果服务器计算机有多个网卡，则计算机默认在所有网卡上进行侦听。您可以通过指定与其中某个网卡绑定的 IP 地址，从而只选择该网卡在配置的端口上进行侦听。

安装过程中，Horizon 7 会对 Windows 防火墙进行配置，打开所需的默认端口。如果要更改端口号或其侦听的网卡，必须手动重新配置 Windows 防火墙以打开更新的端口，以便客户端设备能够连接到服务器。

如果要更改 SSL 端口号，并且需要将 HTTP 重定向，以继续起作用，则您还必须更改 HTTP 重定向端口号。请参阅更改 HTTP 重定向到连接服务器时使用的端口号。

前提条件

确认在此连接服务器实例或安全服务器的外部 URL 中指定的端口在您通过以下步骤更改端口后依然有效。

步骤

1 在连接服务器或安全服务器计算机的 SSL 网关配置文件夹中创建或编辑 `locked.properties` 文件。

例如，*`install_directory`*`\VMware\VMware View\Server\sslgateway\conf\locked.properties`。

`locked.properties` 文件中的属性区分大小写。

2 将 `serverPort` 和/或 `serverPortNonSsl` 属性添加至 `locked.properties` 文件。

例如：

```
serverPort=4443
serverPortNonSsl=8080
```

3 （可选）如果服务器计算机拥有多个网卡，请选择其中一个网卡在已配置的端口上进行侦听。

添加 `serverHost` 和 `serverHostNonSsl` 属性以指定与所指派的网卡绑定的 IP 地址。

例如：

```
serverHost=10.20.30.40
serverHostNonSsl=10.20.30.40
```

通常，SSL 与非 SSL 侦听器都被配置为使用相同的网卡。但如果使用 `serverProtocol=http` 属性来分流客户端连接的 SSL 负载，可以将 `serverHost` 属性设置到单独的网卡，从而为用于启动 Horizon Administrator 的系统提供 SSL 连接。

如果您将 SSL 与非 SSL 连接配置为使用相同的网卡，则 SSL 与非 SSL 端口不能相同。

4 重新启动 Horizon 连接服务器服务或安全服务器服务，使所做的更改生效。

后续步骤

如有必要，手动配置 Windows 防火墙以打开更新的端口。

替换 Horizon 连接服务器实例和安全服务器上 PCoIP 安全网关的默认端口或网卡

您可以替换连接服务器实例或安全服务器上运行的 PCoIP 安全网关服务所使用的默认端口或网卡。贵组织可能要求您执行这些任务以遵循组织策略或避免争用问题。

对于面向客户端的 TCP 和 UDP 连接，PCoIP 安全网关默认在端口 4172 上进行侦听。对于远程桌面的 UDP 连接，PCoIP 安全网关默认在端口 55000 上进行侦听。

本步骤中进行的端口更改不会影响 PCoIP 外部 URL 中指定的端口。根据您的网络配置，可能还需要更改 PCoIP 外部 URL 端口。

如果运行 PCoIP 安全网关的计算机有多个网卡，则它默认对所有网卡进行侦听。您可以通过指定与其中某个网卡绑定的 IP 地址，从而只选择该网卡在配置的端口上进行侦听。

前提条件

确认在连接服务器实例或安全服务器上的 PCoIP 外部 URL 中指定的端口在您通过以下步骤更改端口后依然有效。

步骤

1 在运行 PCoIP 安全网关的连接服务器或安全服务器计算机上启动 Windows 注册表编辑器。

2 导航至 `HKEY_LOCAL_MACHINE\SOFTWARE\Teradici\SecurityGateway` 注册表项。

3 在该注册表项下，使用更新的端口号添加一个或多个以下字符串 (REG_SZ) 值。

例如：

```
ExternalTCPPort "44172"
ExternalUDPPort "44172"
InternalUDPPort "55111"
```

4 （可选）如果运行 PCoIP 安全网关的计算机有多个网卡，请选择一个网卡在已配置的端口上进行侦听。

在同一注册表项下，添加以下字符串 (REG_SZ) 值以指定与所指派的网卡绑定的 IP 地址。

例如：

```
ExternalBindIP "10.20.30.40"
InternalBindIP "172.16.17.18"
```

如果将外部和内部连接配置为使用相同的网卡，则外部和内部 UDP 端口不能相同。

5 重新启动 VMware Horizon View PCoIP 安全网关服务，使所做更改生效。

替换连接服务器实例和安全服务器上 PCoIP 安全网关的默认控制端口

您可以替换用于控制在连接服务器实例或安全服务器上运行的 PCoIP 安全网关 (PCoIP Secure Gateway, PSG) 服务的默认端口。您可能需要执行此任务，以避免出现端口争用情况。

默认情况下，PCoIP 安全网关侦听本地 TCP 端口 50060 上的控制连接。

步骤

1 在正在运行 PCoIP 安全网关的连接服务器实例或安全服务器计算机上的 SSL 网关配置文件夹中创建或编辑 `locked.properties` 文件。

例如，*install_directory*\VMware\VMware View\Server\sslgateway\conf\locked.properties。

`locked.properties` 文件中的属性区分大小写。

2 将 `psgControlPort` 属性添加到 `locked.properties` 文件中。

例如：

```
psgControlPort=52060
```

3 在相同的虚拟机上启动 Windows 注册表编辑器。

4 导航至 HKEY_LOCAL_MACHINE\SOFTWARE\Teradici\SecurityGateway 注册表项。

5 在此注册表项下，使用更新的端口号添加以下 String (REG_SZ) 值。

例如：

```
TCPControlPort "52060"
```

注 TCPControl Port 的端口号与 psgControlPort 的端口号相同。

6 重新启动 Horizon 连接服务器服务或安全服务器服务，使所做的更改生效。

替换 View Composer 的默认端口

默认情况下，View Composer 服务使用的 SSL 证书与特定端口绑定。可以使用 SviConfig ChangeCertificateBindingPort 实用程序替换默认端口。

使用 SviConfig ChangeCertificateBindingPort 实用程序指定新端口时，该实用程序会从当前端口取消 View Composer 证书的绑定，然后将其绑定到新端口。

安装过程中，View Composer 会对 Windows 防火墙进行配置，打开所需的默认端口。如果要更改端口，则必须手动重新配置 Windows 防火墙，使其打开更新的端口，并确保与 View Composer 服务正常连接。

前提条件

确认指定的端口可用。

步骤

1 停止 View Composer 服务。

2 在安装了 View Composer 的 Windows Server 主机上，打开命令提示符。

3 导航到 SviConfig 可执行文件。

该文件与 View Composer 应用程序位于同一位置。默认路径为 C:\Program Files (x86)\VMware\VMware View Composer\sviconfig.exe。

4 键入 SviConfig ChangeCertificateBindingPort 命令。

例如：

```
sviconfig –operation=ChangeCertificateBindingPort
          –Port=端口号
```

其中 –port=*port number* 是 View Composer 将证书绑定到的新端口。–port=*port number* 参数是必需的。

5 重新启动 View Composer 服务，使所做更改生效。

后续步骤

如有必要，可以手动重新配置 View Composer Server 上的 Windows 防火墙，以打开更新的端口。

更改 HTTP 重定向到连接服务器时使用的端口号

如果要替换 Horizon 7 Server 中的默认端口 443，并希望允许试图连接至端口 80 的 Horizon Client 进行 HTTP 重定向，则必须在 Horizon 7 Server 中配置 `locked.properties` 文件。

注　如果将 SSL 负载分流到中间服务器，则本步骤将无效。完成 SSL 负载分流后，Horizon 7 Server 中的 HTTP 端口将向客户端提供服务。

前提条件

请确认是否更改了默认端口号 443。如果使用在安装期间配置的默认值，则无需执行本步骤来保留 HTTP 重定向规则。

步骤

1 在连接服务器或安全服务器计算机的 SSL 网关配置文件夹中创建或编辑 `locked.properties` 文件。

例如，*install_directory*\VMware\VMware View\Server\sslgateway\conf\locked.properties。

`locked.properties` 文件中的属性区分大小写。

2 向 `locked.properties` 文件添加以下行：

```
frontMappingHttpDisabled.1=5:*:moved:https::port
frontMappingHttpDisabled.2=3:/error/*:file:docroot
frontMappingHttpDisabled.3=1:/admin*:missing
frontMappingHttpDisabled.4=1:/view-vlsi*:missing
```

在上述行中，变量 *port* 是客户端应当连接的端口号。

如果不添加上述行，则 *port* 保持为 443。

3 重新启动 Horizon 连接服务器服务或安全服务器服务，使所做的更改生效。

防止客户端连接的 HTTP 重定向到连接服务器

如果 Horizon Client 尝试通过 HTTP 连接到 Horizon 7 Server，则会以静默方式重定向到 HTTPS。在有些部署中，可能需要防止用户在 Web 浏览器中输入 **`http://`**，而应强制用户使用 HTTPS。要防止 Horizon Client 的 HTTP 重定向，必须在 Horizon 7 Server 中配置 `locked.properties` 文件。

注　如果将 SSL 负载分流到中间服务器，则本步骤将无效。完成 SSL 负载分流后，Horizon 7 Server 中的 HTTP 端口将向客户端提供服务。

步骤

1 在连接服务器或安全服务器计算机的 SSL 网关配置文件夹中创建或编辑 `locked.properties` 文件。

例如，*install_directory*\VMware\VMware View\Server\sslgateway\conf\locked.properties。

`locked.properties` 文件中的属性区分大小写。

2 向 `locked.properties` 文件添加以下行：

```
frontMappingHttpDisabled.1=5:*:missing
frontMappingHttpDisabled.2=3:/error/*:file:docroot
```

3 重新启动 Horizon 连接服务器服务或安全服务器服务，使所做的更改生效。

对连接服务器上的 Horizon 7 性能计数器启用远程访问

Horizon 7 性能计数器在连接服务器本地可供查看，但是从其他计算机访问时却返回 0。要对连接服务器上的 Horizon 7 性能计数器启用远程访问，您必须在注册表中配置连接服务器的框架端口。

步骤

1 启动 Windows 注册表编辑器。

2 导航到 `HKEY_LOCAL_MACHINE\SOFTWARE\VMware, Inc.\VMware VDM\Node Manager` 注册表项。

3 添加新的字符串 (REG_SZ) 值 `Management Port`。

4 将 `Management Port` 值设置为 **32111**。

调整 Windows Server 设置以支持您的部署

为支持大规模远程桌面部署，您可以对安装连接服务器的 Windows Server 计算机进行配置。您可以在每个计算机上调整 Windows 页面文件的大小。

默认情况下，Windows Server 2008 R2 和 Windows Server 2012 R2 计算机上的短周期端口、TCB 哈希表和 Java 虚拟机设置均已经过调整。这些调整可确保计算机拥有充足的资源，可在预期的用户负载下正常运行。

调整 Horizon 连接服务器的内存大小

在连接服务器计算机上，部署 50 个或更多远程桌面需要 10 GB 的内存。至少有 10 GB 内存的 Windows Server 计算机会自动进行配置，以支持约 2,000 个并发安全加密链路会话（即，连接服务器能够支持的最大数量）。

仅为小规模的概念验证部署配置小于 10 GB 的内存。如果是 4GB 的最低必需内存，则配置可以支持约 500 个并发安全加密链路会话，这一数量足以支持小型、概念证明型部署。

但是，由于您的部署会随着更多用户加入到环境中而逐渐增大，因此 VMware 建议您始终配置至少 10GB 的内存。唯一的特例是您知道环境大小将不再增加并且无法获得内存时。

如果在内存小于 10 GB 的情况下安装连接服务器，则 Horizon 7 会在安装完成后生成警告消息，以提供内存大小建议。每 12 小时即触发一个事件，该事件说明连接服务器实例配置了少量的物理内存。

如果将计算机内存增加到 10 GB 以支持更大规模的部署，应重新启动连接服务器，以确保 JVM 堆大小自动增加到建议的值。您无需重新安装连接服务器。

重要 请勿更改 64 位 Windows Server 计算机上的 JVM 堆大小。更改该值可能会使连接服务器的行为变得不稳定。在 64 位计算机上，连接服务器服务会将 JVM 堆大小设置为与物理内存相符。

有关连接服务器的其他硬件和内存要求，请参阅 Horizon 连接服务器的硬件要求。

有关在大型部署中使用连接服务器的硬件和内存建议，请参阅《Horizon 7 架构规划指南》中的“连接服务器最高配置和虚拟机配置”。

配置系统页面文件设置

您可以在安装了连接服务器实例的 Windows Server 计算机上更改系统页面文件设置以优化虚拟内存。

安装 Windows Server 后，Windows 会根据计算机的物理内存计算页面文件的初始大小和最大大小。重新启动计算机后，这些默认值设置将保持不变。

如果 Windows Server 计算机是一个虚拟机，您可以通过 vCenter Server 来修改内存大小。然而，如果 Windows 使用默认设置，系统页面文件的大小就不会根据新的内存大小进行调整。

步骤

1 在安装了连接服务器的 Windows Server 计算机上，导航至“虚拟内存”对话框。

默认情况下，**自定义大小**选项会被选中，并会显示页面文件大小的初始大小和最大大小。

2 单击**系统管理的大小**。

Windows 会根据当前的内存使用情况和可用内存空间，不断重新计算系统页面文件的大小。

配置事件报告

11

您可以创建事件数据库来记录有关 Horizon 7 事件的信息。此外，如果您使用 Syslog 服务器，则可以对连接服务器进行配置，使其向 Syslog 服务器发送事件或创建以 Syslog 格式编写的事件平面文件。

本章讨论了以下主题：

- 为 Horizon 7 事件添加数据库和数据库用户
- 为事件报告准备 SQL Server 数据库
- 配置事件数据库
- 为 Syslog 服务器配置事件日志记录

为 Horizon 7 事件添加数据库和数据库用户

您可以通过将事件数据库添加到现有数据库服务器，从而创建一个事件数据库。然后就可以用企业级报告软件来分析数据库中的事件。

在专用服务器上部署事件数据库的数据库服务器，以便事件日志记录活动不会影响置备和对 Horizon 7 部署比较重要的其他活动。

注　您无需为此数据库创建 ODBC 数据源。

前提条件

- 确认在连接服务器实例可访问的系统上具有支持的 Microsoft SQL Server 或 Oracle 数据库服务器。有关支持的数据库版本列表，请参阅 View Composer 和事件数据库的数据库要求。
- 确认您拥有在数据库服务器上创建数据库和用户所需的数据库特权。
- 如果您不熟悉在 Microsoft SQL Server 数据库服务器上创建数据库的过程，请参阅将 View Composer 数据库添加到 SQL Server 中介绍的步骤。
- 如果您不熟悉在 Oracle 数据库服务器上创建数据库的过程，请参阅将 View Composer 数据库添加到 Oracle 12c 或 11g 中介绍的步骤。

步骤

1　向服务器中添加一个新的数据库，并为其提供一个描述性名称，如 HorizonEvents。

　　对于 Oracle 12c 或 11g 数据库，还需要提供 Oracle 系统标识符 (SID)，当您在 Horizon Administrator 中配置事件数据库时将使用该标识符。

2 为该数据库添加一个用户，该用户应具有创建表、视图以及在 Oracle 中创建触发器和序列的权限，并具有读写这些对象的权限。

   对于 Microsoft SQL Server 数据库，不要使用集成 Windows 身份验证 (Integrated Windows Authentication) 安全模式方法进行身份验证。一定要使用 SQL Server 身份验证 (SQL Server Authentication) 方法进行身份验证。

随即会创建数据库，但在 Horizon Administrator 中配置数据库之前不会安装模式。

后续步骤

按照配置事件数据库中的说明操作。

为事件报告准备 SQL Server 数据库

您必须先配置正确的 TCP/IP 属性并确认 Microsoft SQL Server 使用了 SQL Server 身份验证，然后才能使用 Horizon Administrator 在该服务器上配置事件数据库。

前提条件

- 为事件报告创建一个 SQL Server 数据库。请参阅为 Horizon 7 事件添加数据库和数据库用户。
- 确认您拥有配置数据库所需的数据库特权。
- 确认数据库服务器使用 SQL Server 身份验证方法。不要使用 Windows 身份验证。

步骤

1 打开 SQL Server Configuration Manager 并展开 **SQL Server *YYYY* 网络配置**。

2 选择 ***server_name* 使用的协议**。

3 在协议列表中，右键单击 **TCP/IP** 并选择**属性**。

4 将**已启用**属性设置为**是**。

5 确认已分配了一个端口，或者在必要时分配一个端口。

   有关静态和动态端口以及如何分配端口的信息，请参阅 SQL Server Configuration Manager 的联机帮助。

6 确认该端口未被防火墙阻止。

后续步骤

使用 Horizon Administrator 将数据库连接到连接服务器。按照配置事件数据库中的说明操作。

配置事件数据库

事件数据库会将有关 Horizon 7 事件的信息存储为数据库记录，而不是日志文件记录。

安装连接服务器实例后，您便可以配置事件数据库。您只需要在连接服务器组中配置一个主机。组中剩余的主机会自动进行配置。

注　确保连接服务器实例与外部数据库之间的数据库连接安全是管理员的职责，但事件流量仅限于有关 Horizon 7 环境运行状况的信息。如果想采取额外的预防措施，可以通过 IPSec 或其他途径保护此通道的安全，也可以在连接服务器计算机本地部署数据库。

您可使用 Microsoft SQL Server 或 Oracle 数据库报告工具检查数据库表中的事件。有关更多信息，请参阅《Horizon 7 集成指南》文档。

您还可以生成 Syslog 格式的 Horizon 7 事件，以便第三方分析软件能够访问事件数据。您可以使用带 –I 选项的 vdmadmin 命令以 Syslog 格式在事件日志文件中记录 Horizon 7 事件消息。请参阅《Horizon 7 管理指南》文档中的“使用 -I 选项生成 Syslog 格式的 Horizon 7 事件日志消息”。

前提条件

配置事件数据库时需要以下信息：

- 数据库服务器的 DNS 名称或 IP 地址。
- 数据库服务器的类型：Microsoft SQL Server 或 Oracle。
- 用来访问数据库服务器的端口号。适用于 Oracle 的默认端口号是 1521；适用于 SQL Server 的默认端口号是 1433。对于 SQL Server，如果数据库服务器是已经命名的实例，或者您使用的是 SQL Server Express，您可能需要确定端口号。有关连接到已命名的 SQL Server 实例的信息，请参阅 http://support.microsoft.com/kb/265808 上的 Microsoft 知识库文章。
- 您在数据库服务器上创建的事件数据库名称。请参阅为 Horizon 7 事件添加数据库和数据库用户。

  对于 Oracle 12c 或 11g 数据库，在 Horizon Administrator 中配置事件数据库时，必须使用 Oracle 系统标识符 (SID) 作为数据库名称。
- 为该数据库创建的用户的用户名和密码。请参阅为 Horizon 7 事件添加数据库和数据库用户。

  为该用户使用 SQL Server 身份验证 (SQL Server Authentication)。不要使用集成 Windows 身份验证 (Integrated Windows Authentication) 安全模式方法进行身份验证。
- 事件数据库中表的前缀，如 VE_。通过添加前缀，可在安装的 Horizon 7 之间共享数据库。

  注　您必须输入对当前使用的数据库软件有效的字符。填写完对话框时不会对前缀语法进行检查。如果输入的字符对当前使用的数据库软件无效，则当连接服务器尝试连接数据库服务器时将会出现错误。日志文件会提示所有错误，其中包括该错误和数据库名称无效时从数据库服务器返回的任何其他错误。

步骤

1　在 Horizon Administrator 中，选择 **View 配置 > 事件配置**。

2　在**事件数据库**区域中，单击**编辑**，然后在提供的字段中输入信息，最后单击**确定**。

3 （可选）在”事件设置“窗口中，单击**编辑**，分别更改事件的显示时间长度以及将事件归为新事件的天数，然后单击**确定**。

这些设置可控制事件在 Horizon Administrator 界面中显示的时间长度。在此之后，事件仅在历史数据库表中可见。

”数据库配置“窗口可显示事件数据库的当前配置。

4 选择**监视 > 事件**，确认已成功连接到事件数据库。

如果连接失败，则会显示错误消息。如果您使用 SQL Express 或命名的 SQL Server 实例，您可能需要确定正确的端口号，如前提条件中提到的端口号。

在 Horizon Administrator 控制板中，“系统组件状态”的“报告数据库”标题下会显示事件数据库服务器。

为 Syslog 服务器配置事件日志记录

您可以生成 Syslog 格式的 Horizon 7 事件，以便分析软件能够访问事件数据。

您只需要在连接服务器组中配置一个主机。组中剩余的主机会自动进行配置。

如果启用基于文件的事件日志记录，则事件会在本地日志文件中累积。如果指定文件共享，这些日志文件将移至该共享中。

- 仅在配置期间进行快速故障排除时（可能在配置事件数据库之前）使用本地文件，这样就有办法查看事件。

  在删除最早的文件之前，事件日志记录的本地目录最大（包含已关闭的日志文件）为 300MB。Syslog 输出的默认目标位置为 `%PROGRAMDATA%\VMware\VDM\events\`。

- 对于时间很长的事件记录，或者如果您没有 Syslog 服务器，或者当前的 Syslog 服务器无法满足您的要求，请使用 UNC 路径保存日志文件。

您也可以使用 `vdmadmin` 命令以 Syslog 格式配置基于文件的事件日志记录。请参阅《Horizon 7 管理指南》文档中有关使用 `vdmadmin` 命令的 `-I` 选项生成 Syslog 格式的 Horizon 7 事件日志消息的主题。

重要 Syslog 数据在不采用软件加密的情况下跨网络传输，它可能包含敏感数据，例如用户名。VMware 建议使用链路层安全机制（例如 IPSEC）来避免这类数据在网络上受到监视。

前提条件

配置连接服务器时需要使用以下信息，以便能以 Syslog 格式记录事件和/或将事件发送到 Syslog 服务器：

- 如果您计划使用 Syslog 服务器侦听 UDP 端口上的 Horizon 7 事件，您必须具有 Syslog 服务器的 DNS 名称或 IP 地址以及 UDP 端口号。默认 UDP 端口号为 514。
- 如果您计划以平面文件格式收集日志，则必须拥有指向存有日志文件的文件共享和文件夹的 UNC 路径，同时还必须具备有权对文件共享执行写入操作的帐户的用户名、域名和密码。

步骤

1 在 Horizon Administrator 中，选择 **View 配置 > 事件配置**。

2 （可选）在 **Syslog** 区域，要将连接服务器配置为向 Syslog 服务器发送事件，请单击**发送到 syslog 服务器**旁边的**添加**，然后提供服务器名称或 IP 地址以及 UDP 端口号。

3 （可选）要以 Syslog 格式生成 Horizon 7 事件日志消息并将其存储在日志文件中，请选中**记录到文件: 启用**复选框。

如果不指定文件共享的 UNC 路径，日志文件会保留在本地。

4 （可选）要将 Horizon 7 事件日志消息存储在文件共享中，请单击**复制到位置**旁边的**添加**，然后提供文件共享的 UNC 路径和用于存储日志文件的文件夹，以及具有文件共享写入权限的帐户的用户名、域名和密码。

以下是 UNC 路径示例：

```
\\syslog-server\folder\file
```